United States General Accounting Office

GAO

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

September 2003

ELECTRONIC GOVERNMENT

Planned e-Authentication Gateway Faces Formidable Development Challenges

GAO-03-952

September 2003

ELECTRONIC GOVERNMENT

Planned e-Authentication Gateway Faces Formidable Development Challenges

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-952, a report to the Committee on Government Reform and the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House of Representatives

Why GAO Did This Study

For on-line government services that involve sensitive information, such as financial or personal information, it is important to be able to confirm the identity of potential users. This confirmation process, known as authentication, is crucial for security and user confidence. The General Services Administration (GSA) is developing an "e-Authentication gateway," which is to provide a consolidated electronic authentication service to support the e-government initiatives sponsored by the Office of Management and Budget (OMB). The figure depicts schematically how the gateway process would work. GAO was asked to (1) assess GSA's progress in implementing the proposed initiative and (2) identify the challenges associated with implementing the gateway.

What GAO Recommends

GAO recommends that the Administrator of GSA, in conjunction with OMB, take steps to ensure that e-Authentication gateway implementation challenges are fully addressed, including, among other things, revising the schedule for deploying a fully operational version of the gateway and working to define key technical interfaces to promote interoperability with commercial products.

In commenting on a draft of this report, agency officials requested that we include updated information, which has been incorporated in this report.

www.gao.gov/cgi-bin/getrpt?GAO-03-952.

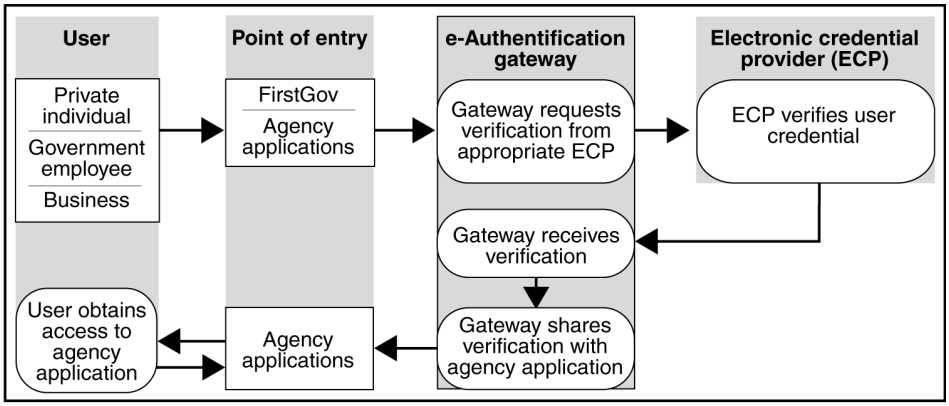
To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

What GAO Found

Although the original goal was for the e-Authentication gateway to be operational by September 2003, GSA has achieved few of its project objectives and recently extended the milestone for completing a fully operational system to March 2004. GSA has completed several important tasks, such as issuing a request for information and fielding a demonstration prototype of the gateway. However, other essential activities, such as developing authentication profiles—requirements summaries that address the needs of the other 24 OMB e-government initiatives—have not yet been fully addressed. Further, to meet the new milestone, GSA plans to compress the acquisition process for the operational gateway by awarding a contract by December 2003 for delivery of an operational gateway by March 2004. This accelerated schedule may be difficult to achieve. The modest progress achieved to date calls into question the likelihood that the project can successfully field an operational gateway, even within the revised schedule.

The challenges facing the e-Authentication gateway project make it difficult for GSA to achieve the kind of rapid results envisioned for the initiative. For example, procedures and guidance have not yet been completed defining the specific technologies to support different authentication requirements. In addition, technical standards have not yet been agreed upon to provide a basis for ensuring interoperability among different authentication products and systems. Further, GSA has not taken full measures to ensure that the gateway system is adequately secured and that privacy information is adequately protected. Addressing these and other challenges is essential to the successful deployment of a gateway that can effectively support the authentication requirements of OMB's e-government initiatives.

Overview of e-Authentication Gateway Process



Source: GAO analysis of e-Authentication Gateway process.

Contents

Letter 1

Results in Brief 2
Background 4
Objectives, Scope, and Methodology 10
Important Objectives and Milestones Have Not Been Fully Met 11
Formidable Challenges Hinder Speedy Deployment of an Operational Gateway 15
Conclusions 24
Recommendations for Executive Action 24
Agency Comments and Our Evaluation 25

Appendixes

Appendix I: Comments from the General Services Administration 27

Appendix II: Comments from the Department of Commerce 29

Glossary 32

Figure

Figure 1: Using the e-Authentication Gateway 9

Abbreviations

API	application-programming interface
CIO	chief information officer
e-RA	e-Authentication requirements and risk analysis
ECP	electronic credential provider
FBCA	Federal Bridge Certification Authority
GPEA	Government Paperwork Elimination Act
GSA	General Services Administration
MOU	memorandum of understanding
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIN	personal identification number
PKI	public-key infrastructure
RFI	request for information
RFP	request for proposal

Contents

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

September 12, 2003

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives

The Honorable Adam H. Putnam
Chairman, Subcommittee on Technology, Information Policy,
Intergovernmental Relations, and the Census
Committee on Government Reform
House of Representatives

Many government services depend on transactions that exchange sensitive information, such as financial or personal information. As the federal government strives to deliver more services on-line, it increases the need to safeguard electronic transactions involving such information. Both the electronic system and the user need assurance that the user's identity can be confirmed: the system needs to know that the user is authorized to exchange the information, which in turn allows the user to have some confidence that the system will not release sensitive information to unauthorized users. This confirmation of user identity is known as authentication.

Systems perform authentication by examining electronic credentials[1] provided by users and determining their trustworthiness. Such credentials can be generated through a variety of technologies and provide differing levels of assurance, depending on the type of technology used and whether the system is properly implemented and maintained. Establishing an on-line environment of systems with the capability to verify a wide range of credentials is essential to maintaining public confidence in the government's ability to conduct business over the Internet and protect confidential information from unauthorized access.

[1]Electronic credentials are the electronic equivalent of traditional paper-based credentials—documents that vouch for an individual's identity.

This report responds to your request that we assess the progress of the General Services Administration (GSA) in implementing its e-Authentication initiative and the challenges associated with developing the e-Authentication gateway, which is the centerpiece of the initiative. The e-Authentication gateway is being developed to provide a consolidated electronic authentication service to support 24 major electronic government (e-government)[2] initiatives sponsored by the Office of Management and Budget (OMB). All these initiatives, including e-Authentication, were originally chosen by OMB in part because of the likelihood of their being deployed within 18 to 24 months. In this regard, we agreed to (1) assess GSA's progress in implementing the proposed initiative and (2) identify the challenges associated with implementing the gateway.

Results in Brief

OMB originally set a goal for the e-Authentication gateway to be operational by September 2003, but GSA has thus far achieved few of its project objectives, and OMB recently extended the milestone for completing a fully operational system to March 2004. While important tasks—such as issuing a request for information (RFI) and fielding a demonstration prototype of the gateway—were completed, other activities essential to the successful deployment of an operational gateway, such as establishing authentication profiles for the 24 e-government initiatives, have not yet been fully addressed. Further, to meet the new milestone, GSA plans to compress the acquisition process for the operational gateway by awarding a contract by December 2003 for delivery of an operational gateway by March 2004. This accelerated schedule may be difficult to achieve. Fielding a fully operational gateway without a full consideration of technical options increases the risk that the gateway will not work as intended, support user requirements, or receive financial support from partner agencies. The modest progress achieved to date calls into question the likelihood that the project can successfully field an operational gateway, even within the revised schedule.

While the gateway has the potential to provide multiple benefits to the other 24 e-government initiatives and the public, several formidable challenges will make it difficult for GSA to achieve the kind of rapid results

[2]E-government refers to the use of technology, particularly Web-based Internet applications, to enhance the access to and delivery of government information and services to citizens, business partners, employees, and other entities.

envisioned by OMB for the initiative. These challenges include the following:

- *Establishing comprehensive policies and guidance*. Comprehensive policies and procedures to promote consistency and interoperability among disparate authentication systems operating across the federal government have not yet been completed, making it difficult for federal agencies developing the 24 e-government initiatives to make decisions on what types of authentication technologies and systems to implement.

- *Defining user authentication requirements*. User requirements have not yet been fully defined, and as of August 2003, assessments had been conducted for 12 of the 24 e-government initiatives to determine their authentication needs and appropriate assurance levels. GSA has not been considering the results of these risk assessments in designing the gateway.

- *Achieving interoperability*[3] *among available authentication products*. Technical standards have not yet been agreed upon to provide a basis for ensuring interoperability among different authentication products and systems.

- *Fully addressing funding, security, and privacy issues*. GSA has not developed an effective investment strategy to support full-scale development of the gateway or taken full measures to ensure that the gateway system is adequately secured and that privacy information is adequately protected.

Addressing these challenges is essential to the successful deployment of a gateway that can effectively support the authentication requirements of the 24 e-government initiatives. In light of these challenges, we are making recommendations to the Administrator of GSA aimed at improving planning and systems development activities now under way and at coordinating activities with other federal agencies to better ensure that the gateway provides robust support for multiple authentication requirements based on a range of commercial products. We also are making recommendations that OMB work with GSA, in conjunction with the National Institute of Standards and Technology (NIST) and the federal

[3]Interoperability is the ability of two or more systems or components to exchange information and to use the information that has been exchanged.

Chief Information Officers (CIO) Council, to expand and improve e-Authentication policies and guidance to meet the needs of an operational gateway.

We received written comments on a draft of this report from the Administrator of GSA and from the Secretary of Commerce. We also received oral comments from staff of OMB's Office of General Counsel. GSA generally agreed with our discussion of the challenges hindering speedy deployment of the e-Authentication gateway, as well as our recommendations aimed at addressing these challenges. The agency requested that we include more information on recent developments, which we have incorporated in this report. OMB staff said the agency agreed with GSA's comments. NIST officials generally agreed with the content of information and recommendations in the draft report and requested that we update information on recently drafted authentication guidance. We updated this report accordingly.

Background

To deliver complete on-line services to citizens, business partners, employees, and other entities, the government needs to authenticate the identity of users who wish to conduct transactions involving sensitive information, such as financial or personal information. A variety of authentication technologies are in use, providing differing levels of assurance, depending on the type of technology and whether the system is properly implemented and maintained. Establishing an electronic gateway with the capability to verify a wide range of credentials is a critical element in the federal government's strategy for maintaining public confidence in the conduct of public business over the Internet and protecting confidential information from unauthorized access. It is also consistent with the government's effort to integrate information technology investments across agencies and to streamline services.

A Variety of Techniques Are Used to Perform Authentication

The electronic authentication process can involve a range of different technologies and electronic credentials, each with varying strengths and weaknesses in ensuring that parties are who they claim to be when conducting electronic transactions. The types of identifying factors used by these different technologies can generally be grouped into three basic categories: (1) "something you know," such as a password; (2) "something you have," such as a smart card or other token; and (3) "something you are," including biometric identifiers such as fingerprints or retina scans.

- *Something you know*: An authentication process based on "something you know" relies on information known by both the user and the system—a "shared secret"—and offers some advantages and disadvantages. The most common types of shared secrets are passwords and personal identification numbers (PIN), which are used by systems to confirm the identity of individuals accessing computers. Users wishing to access such a system are required to enter a password when they first turn on and log into the system, confirming the shared secret. Systems that support password-based authentication processes are relatively easy to implement, because they do not require external products or specialized devices. However, they provide only relatively limited confidence in the identity of users, because users often share their secret codes with others or select common phrases and dates that others can easily identify or guess.

- *Something you have*: An authentication system based on "something you have" relies on physical devices—such as smart cards or other physical tokens—or tamper-resistant electronic credentials, such as digital certificates. Physical devices are encoded with information that can verify the identity of the device's owner. To initiate the authentication process, a user inserts a token or smart card into an electronic reader, and the system verifies information stored on the device. Electronic credentials, such as digital certificates, can be either stored on a smart card or token and accessed through a reader or stored in a user's computer. Digital certificates are small electronic files containing identifying information that is encrypted to be tamper-resistant. Public-key infrastructure (PKI) is a prominent security technology that makes use of digital certificates for authentication and may also involve the use of a physical device or token.[4]

[4]A PKI is a system of hardware, software, policies, and people that can provide a set of information assurances, including authentication, that are important in conducting electronic transactions. For more information on PKI, 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).

- *Something you are*: Authentication systems based on "something you are" use biometric technologies to capture measurements of personal characteristics—such as fingerprints, hands, or facial features—to authenticate users. Characteristics from individuals are measured and averaged to create unique digital representations of these characteristics, called templates, that are stored centrally in a database or locally in a user's token, such as a smart card. The user must present the characteristic, such as a finger or hand, to the authentication device to gain access to the system. The device then compares the stored template to the live characteristic of the individual for verification. If the characteristics match, the user is authenticated and allowed to access the system. Biometric technologies have the advantage of not requiring that an individual remember a shared secret or keep track of a physical authentication device, although biometrics are often used in combination with at least one of the other factors.[5]

The technologies used to exploit these three authentication factors can be combined and implemented in many different ways to provide different levels of assurance. For example, a Web site that requires users to enter a password provides only very limited assurance of the identity of individuals who successfully log on with a correct password. A more sophisticated system that requires users to insert a smart card and also enter a PIN likely will provide a greater level of assurance, because it would be much harder for an imposter to gain access to both the smart card and the PIN required to successfully impersonate a legitimate user. A system requiring users to provide a biometric identifier in addition to a smart card and PIN would arguably offer an even higher level of assurance that users were indeed who they claimed to be.[6]

[5]For more information on biometrics, see U.S. General Accounting Office, *Technology Assessment: Using Biometrics for Border Security,* GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

[6]This discussion assumes that each of these hypothetical systems has been properly implemented and maintained. The level of assurance provided by any specific system is dependent on how well the system has been implemented and maintained. Further, a system's ability to successfully authenticate a given user does not provide direct assurance that the user's data are secure and reliable, because the user's system could have security weaknesses unrelated to user authentication.

More sophisticated authentication techniques can have some drawbacks. For example, biometric devices tend to be expensive and must be deployed at all locations where users need to access systems. Further, as we reported previously,[7] users tend to resist having to present physical characteristics for authentication. As a result, care must be taken to choose an appropriate level of authentication for any given system, based on an examination of the costs of the systems and the risks of information being compromised. Federal government systems can be expected to include a broad range of applications requiring a variety of assurance levels.

Gateway Established to Provide Common, Governmentwide Authentication Services

In October 2001, the President's Management Council, working with OMB, endorsed the development of 24 e-government initiatives[8] to significantly improve the delivery of services to citizens across government. OMB set a goal for initial capabilities to be achieved for each of the initiatives by September 2003. The objective of the e-Authentication initiative was to provide a centralized gateway to verify the identity of users, based on multiple types of credentials, in support of the other e-government initiatives. By accommodating different and multiple authentication mechanisms—such as passwords, tokens, digital certificates, and biometrics—the gateway was intended to support the different levels of assurance that are likely to be required for conducting personal or financially sensitive government transactions. In October 2001, OMB tasked GSA to be the managing partner for the e-Authentication initiative. As managing partner, GSA was given responsibility for spearheading the e-Authentication initiative, identifying the authentication requirements of the other 24 e-government initiatives, and completing an operational gateway by September 30, 2003. GSA also was tasked with working with NIST, which is responsible for setting technical standards for the federal government, to develop authentication assurance policies and guidelines, as well as with the federal CIO Council on issues related to the Federal Bridge Certification Authority.[9] As envisioned, the gateway offers multiple

[7]U.S. General Accounting Office, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002), p. 68.

[8]The OMB-sponsored e-government initiatives now number 25. In 2002, a decision was made to separate the e-Clearance initiative from the Integrated Human Resources initiative, resulting in an increase in the number of initiatives from 24 to 25.

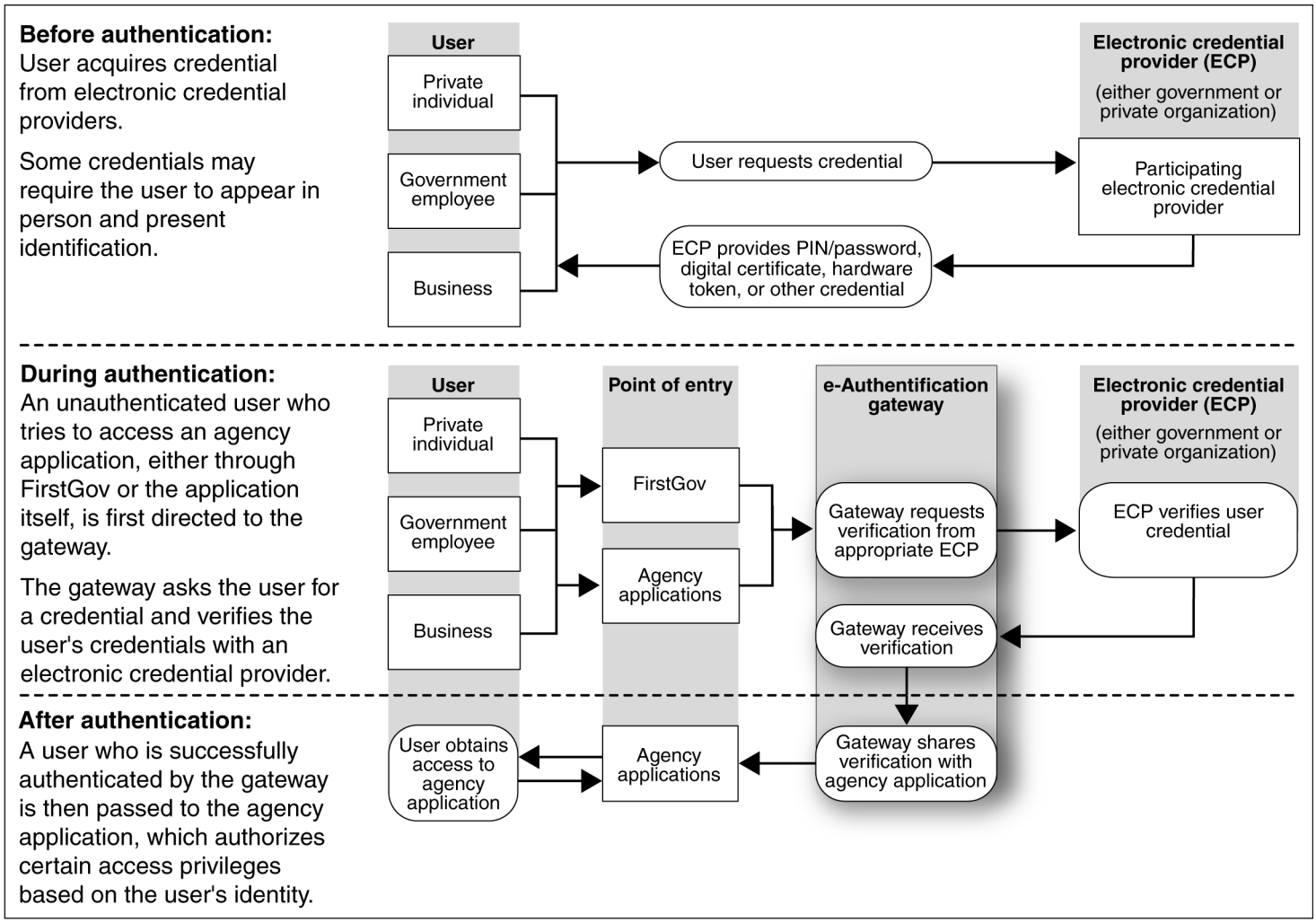
[9]The Federal Bridge Certification Authority, which became operational in June 2001, facilitates PKI-based transactions across agencies.

benefits to citizens and federal agencies conducting on-line transactions, including simplified access to government applications and services and cost savings to agencies through the deployment of common authentication technologies and services.

One of the primary goals of the gateway is to promote secure, easy-to-use methods for users to prove their identity to federal agencies and obtain personal or financially sensitive on-line information and services from these agencies. Other goals include establishing uniform standards for accessing government services while protecting against fraud as much as possible and reducing the need to maintain duplicate credentials and user registration information for multiple government applications and services. In support of these goals, the gateway is to provide what is known as "single sign-on" capability: that is, using one authentication method to verify the identity of a user while granting access to multiple applications and services. Providing single sign-on capability simplifies the authentication process by using the same identification method to verify the identity of users from application to application. Further, the intention is to extend this benefit beyond the 24 e-government initiatives: although the gateway was established to support these initiatives, upon completion, it is intended to be used to support other applications and services across government.

As envisioned, the gateway will provide authentication services through a governmentwide portal and links to agency-level applications. The plan is for users to rely on a governmentwide portal—such as the FirstGov.gov site—to direct them to authentication services offered by the gateway. Users would then be able to present credentials for authentication. Alternatively, users could be directed to the gateway from within specific agency applications to verify their identities before they can access information or services. Once a user's credential has been successfully authenticated, the user will then be granted appropriate access to the application. After being authorized to use a specific application, a user may request access to another application that is also linked to the gateway. If the second application accepts credentials from the user and the first application, no additional authentication will be required. If the second application requires a credential with a higher level of security, the user will have to provide new credentials. Figure 1 provides a schematic diagram of the gateway's planned authentication services.

Figure 1: Using the e-Authentication Gateway



Source: GAO analysis of e-Authentication Gateway process.

Although the gateway will serve as a central point for authentication, it will not issue, maintain, or store credentials. Instead, the gateway will rely on a network of electronic credential providers (ECP), which are to include both government agencies and private sector companies. ECPs will issue credentials after verifying the identities of users based on traditional means—such as the presentation of passports, drivers' licenses, and other identification documents—or by checking standardized databases, such as credit history databases. Users seeking authentication from the gateway

will be directed to appropriate ECPs to obtain credentials if they do not already have them. Delegating the issuing of credentials to ECPs allows the gateway to support a range of credentials and eliminates the need for the gateway to maintain a repository of identification information for all credentialed users. ECPs are to be responsible for all aspects of managing user credentials, including replacing lost or expired credentials and maintaining the identification information associated with the credentials. Agency applications will retain the responsibility to authorize users to conduct specific transactions, such as creating or approving information, based on authenticated credentials.

The gateway has the potential to provide multiple benefits to the other 24 e-government initiatives and to the public. Some of these benefits include standardizing credentials and authentication technologies across government, improving cost savings by eliminating redundant purchases and authentication services, and simplifying public access to multiple government applications and services. The cost savings could be substantial. In its fiscal year 2004 budget plan, GSA estimated that over a 5-year period, gateway costs would total about $73 million, while over the same period, costs for separate authentication systems at individual agencies are estimated to total approximately $460 million. Much of the cost savings from centralizing authentication would also come from reducing the number of passwords that need to be administered from agency to agency and application to application. An official with Gartner,[10] a market research company, provided an indication of the costs associated with resetting lost passwords: in a privately funded study, these were found to total about $50 per event. Finally, the federal government could enhance the willingness of citizens to conduct business electronically by providing centralized authentication services that reduce the burden on citizens of negotiating multiple credentials and authentication systems to access disparate government electronic services.

Objectives, Scope, and Methodology

Our objectives were to (1) assess the progress GSA has made in implementing the e-Authentication gateway and (2) identify key challenges associated with implementing the gateway. To assess GSA's progress in implementing the gateway, we reviewed project plans, cost estimates, funding strategies, contracting activities, testing results, performance

[10]Gartner, Inc., is a research and advisory firm that provides technology-related consulting, research, and other services.

metrics, and other project documentation, including studies completed by GSA, OMB, NIST, and other federal agencies on related authentication and security issues. We also interviewed GSA project managers and officials from other agencies involved in the initiative, such as Agriculture, the Treasury, and the National Aeronautics and Space Administration. Contract employees involved in developing and testing the prototype were also interviewed.

To assess key challenges associated with implementing the proposed e-Authentication gateway, we reviewed and analyzed relevant technical reports and evaluations of authentication technologies and services completed by industry experts and research groups to identify key management and technology issues. We also held discussions with officials responsible for managing the project within GSA, as well as other agency officials involved in development of the prototype. We conducted these discussions with officials from Agriculture's National Finance Center and two large federal agencies—the Departments of Defense and Commerce—to obtain information on funding and technical issues related to the gateway.

We performed our review in accordance with generally accepted government auditing standards, working from November 2002 through July 2003, at various locations, including GSA Headquarters in Washington, D.C; NIST Headquarters in Gaithersburg, Maryland; and the National Finance Center in New Orleans, Louisiana.

Important Objectives and Milestones Have Not Been Fully Met

GSA's drive to make the e-Authentication gateway operational quickly has resulted in few objectives being achieved and changes to planned tasks that have increased project risks. While GSA has completed several important tasks—such as issuing an RFI and fielding a demonstration prototype of the gateway—it has not yet fully addressed objectives essential to the successful deployment of an operational gateway, and it has extended the milestone for making the gateway fully operational from September 2003 to March 2004. To meet the new milestone, GSA plans to compress the acquisition process for making the gateway fully operational by issuing a request for proposal (RFP) and awarding a contract in December 2003. According to the project manager, the contractor will be expected to have a fully operational gateway up and running by the March 2004 milestone. However, this accelerated schedule may be difficult to achieve because it is based on an extremely short time frame, which allows the selected

contractor only 3 months to develop, test, and deploy a fully operational gateway.

In December 2001, GSA developed its original plan for implementing a fully operational e-Authentication gateway. Major tasks included

1. developing and issuing an RFI and RFP to obtain industry input on technical approaches to authentication for potential incorporation into the e-Authentication gateway,

2. assisting e-government initiatives and other federal agencies in identifying their authentication requirements,

3. developing authentication profiles that address the needs of the other 24 e-government initiatives by linking their requirements to a set of standard authentication technologies,

4. enabling three multiuse applications to interoperate with the gateway, and

5. revising existing governmentwide contracting mechanisms for PKI-related services to promote broader use by federal agencies.

To date, GSA has partially addressed four of these five tasks. The first major task—to develop and issue an RFI and RFP—was partially completed in July 2002 with the issuance of an RFI. GSA obtained input from 54 industry representatives on potential technical approaches to implementing e-Authentication in response to the RFI. This information was used to help design the prototype gateway and a framework for delivering authentication services. However, in April 2003, GSA decided to use its existing contractor—builder of the prototype version of the gateway—to continue work aimed at deploying an "interim" operational version of the gateway, and to delay the milestone for the fully operational version of the gateway from September 2003 to March 2004. According to an April 2003 letter from GSA's Chief Information Officer to OMB, the anticipated delay was due to the lack of receipt of funds from federal agency partners. In commenting on a draft of this report, GSA officials further stated that the delay was due to a lack of demand for authentication services from the 24 other e-government initiatives, as well as industry's lack of readiness to provide interoperable gateway services. The e-Authentication project manager told us in July 2003 that GSA planned to compress the acquisition process for the operational gateway by issuing an

RFP, selecting a contractor, and awarding a contract by December 2003. According to the project manager, the contractor would be expected to deploy a fully operational gateway by the March 2004 milestone. (Originally GSA had planned to issue an RFP in September 2002 to have an operational gateway in place a full year later.) Awarding a competitively selected contract is important because it allows a range of alternatives to be considered before a final technical approach is selected. However, the accelerated schedule contemplated by GSA may be difficult to achieve because it is based on an extremely short time frame, which allows the selected contractor only 3 months to develop and deploy a fully operational gateway. In addition, GSA will need time to complete the required certification and accreditation process in order to obtain full authority to operate the gateway.

GSA also partially completed the second task of assisting e-government initiatives and other federal agencies in identifying their authentication requirements. Identifying requirements is important because they represent the blueprint that system developers and program managers use to design, develop, and acquire a system. GSA worked with the Software Engineering Institute[11] to develop an assessment tool to identify authentication requirements by helping agencies determine appropriate assurance levels for their planned electronic transactions. However, the process of identifying requirements is still under way. Thus far, only 12 of the 24 e-government initiatives have completed assessments and shared this information with GSA. Officials plan to conduct assessments for 5 of the other initiatives. According to GSA officials, assessments are not planned for the other 7 initiatives, because those initiatives have no requirements for electronic authentication at this time. Without fully defined requirements, the gateway project faces the risk that extensive or costly changes may be needed before it will meet the needs of all the e-government initiatives.

GSA has also taken steps to address its fourth major task, enabling three e-government applications to interoperate through the gateway. A prototype version of the gateway was fielded on schedule in September 2002. However, the prototype gateway accommodated just one demonstration version of a multiuse application managed by the

[11]The Software Engineering Institute at Carnegie Mellon University is a federally funded research and development center that provides services intended to improve the quality of automated systems and software development and maintenance practices.

Department of Agriculture's National Finance Center. It did not support any of the 24 e-government initiatives. The gateway's project manager said that as of June 30, 2003, the gateway had achieved initial operational capability and was supporting vital records transactions from state and local governments to the Social Security Administration. Approximately 400 transactions had been supported as of July 25, 2003. However, these transactions were also not associated with any of the OMB-sponsored e-government initiatives. Officials said that work was under way to develop a link for the Disaster Management initiative, although no milestone had been set for making that link operational.

According to GSA officials, action has also been taken to address the fifth task—to revise mechanisms for governmentwide contracting for PKI-related services, as a means to promote broader use by federal agencies. Specifically, GSA officials reported that policy for use of its Access Certificates for Electronic Services program had been modified in June 2003 to provide for broader use.

The remaining task (task 3), establishing authentication profiles for the 24 e-government initiatives, has not been addressed, because not all e-government initiatives have yet identified their authentication requirements and because technical guidance for linking those requirements to specific technologies has not yet been finalized by NIST.

In its updated e-government strategy plan, released in April 2003,[12] OMB set milestones for several ongoing gateway-related tasks. These interim milestones included issuing governmentwide authentication guidance by April 2003, deploying the first applications linked to the gateway by May 2003, and establishing a list of credential providers by August 2003. However, these interim tasks have not yet been fully addressed. For example, governmentwide authentication guidance was not issued as planned in April 2003, although OMB partially addressed this objective by issuing a draft version of the guidance for comment in March. No revised time frame has been established for finalizing this guidance. Nor were applications deployed and linked to the gateway in May 2003. The project's milestones were extended because of funding limitations and technical problems, according to the gateway program manager. GSA, which was tasked by OMB to lead the gateway implementation effort, now plans to

[12]Office of Management and Budget, *Implementing the President's Management Agenda for E-Government—E-Government Strategy* (April 2003).

link the first of the 24 e-government initiatives to the gateway in July 2003 rather than May 2003. In addition, GSA now plans to complete the remaining tasks to make the gateway fully operational by March 2004, rather than September 2003.

Formidable Challenges Hinder Speedy Deployment of an Operational Gateway

Developing the e-Authentication gateway has been a challenging undertaking. A variety of technical and management challenges have hindered GSA's progress in developing and deploying the gateway as originally planned. These challenges include establishing comprehensive policies and guidance, fully defining user requirements, achieving interoperability among commercial authentication products, and addressing resource, security, and privacy issues. Addressing these challenges will require the cooperation of federal agencies developing the 24 e-government initiatives, as well as commitment by GSA to making the gateway a fully operational cross-agency resource.

Policies and Guidance Are Not Yet Complete

While GSA has drafted guidance to assist federal agencies in deciding on what types of authentication technologies and systems to implement, policies and procedures to promote consistency and interoperability among disparate authentication systems operating across the federal government have not yet been completed. Policies and procedures are needed to specify such things as the range of standard assurance levels to be supported; the types of authentication technologies appropriate for each of those levels; processes for issuing, maintaining, and revoking electronic credentials; and procedures for ensuring that individual agencies and credential providers are meeting security standards in operating and maintaining their separate systems. Without such standard policies and procedures, agencies are unlikely to develop systems that provide consistent levels of security, which would make it difficult to achieve interoperability across agencies and could lead to security vulnerabilities if authentication systems are not properly designed and implemented.

OMB is responsible for establishing policies, standards, and guidelines for information management, including e-government. In March 2003, OMB published draft guidance on electronic authentication to promote consistent authentication processes across government.[13] The draft guidance proposes four standard assurance levels for authentication, termed "minimal," "low," "substantial," and "high." Examples were provided that were intended to assist agencies in identifying the levels of assurance that would be appropriate for specific applications, based on an assessment of the risks and consequences if transactions were completed in error. According to OMB, the purpose of the guidance, when finalized, is to help federal agencies make consistent decisions about authentication risks, reduce authentication system development and acquisition costs, and minimize the number and type of electronic credentials that federal employees, citizens, and businesses need to conduct electronic transactions with the government. No date has yet been set for completing the draft guidance.[14]

Further, guidance has not been provided to agencies on how to identify appropriate technologies to address their authentication requirements. According to OMB, agencies must first identify the assurance levels associated with their planned e-government transactions and then refer to additional technical guidance to identify appropriate technical implementations. NIST has been tasked with developing this guidance, which would specify the types of technologies that could be used to conduct transactions at each of the OMB-defined assurance levels. A NIST official indicated that an initial draft of this guidance would be available for comment by September 2003. However, until the NIST guidance is completed, technical requirements for the gateway may be difficult to identify, and agencies will be at risk of choosing authentication systems that may need to be changed at a later date to conform to NIST's guidance.

[13]Office of Management and Budget, *Procedures and Guidance on Implementing E-Authentication for Federal Agencies*, Draft Version 15 (Washington, D.C.: Mar. 28, 2003).

[14]For electronic authentication based on PKI technology, in 2000, OMB issued implementation guidance for the Government Paperwork Elimination Act, Public Law 105-277, Div. C, tit. XVII, directing agencies to consider using PKI for (1) transactions in which parties commit to actions or contracts that may give rise to financial or legal liability and (2) transactions that involve the transfer of funds. See Office of Management and Budget, *Procedures and Guidance on Implementing the Government Paperwork Elimination Act*, Memorandum M-00-10 (Apr. 25, 2000), pp. 19–20.

In addition to OMB and NIST guidance setting standard authentication levels and associated technology alternatives, additional policy and procedures covering other aspects of administering e-Authentication consistently across the government have not been completed. In July 2003, GSA issued a draft framework for evaluating the processes used by ECPs to issue credentials to users for conducting transactions at each of the four assurance levels. Agencies need to be able to assess compliance with standard policies and procedures in order to be able to determine whether the credentials issued and managed by specific ECPs have an adequate degree of trustworthiness. GSA also drafted guidance in July 2003 for the use of passwords, PINs, and PKI. However, no milestones have been set for finalizing this guidance. In other areas, no guidance has been developed. Guidance concerning authorization—the process of granting appropriate access privileges to authenticated users—is an example. A GSA official indicated that such guidance could help ensure that agencies perform authorization consistently across government. However, GSA officials said they had no plans to develop authorization guidance, because they considered authorization to be the responsibility of the agencies that control the software applications being supported.

User Authentication Requirements Have Not Been Fully Defined

In addition to the lack of complete policies and procedures, implementation of the e-Authentication gateway is also impeded by the lack of defined authentication requirements from the other 24 e-government initiatives and agencies expected to use the gateway. Improperly defined or incomplete requirements have often been identified as a root cause of the failure of systems to meet their cost, schedule, or performance goals.[15] Key stakeholders and other federal agencies responsible for e-government initiatives and for contributing funding for the gateway have not been involved in assessing the prototype and determining whether it is suitable for operational deployment.[16] According to a GSA project official, the 24 e-government initiatives have played a

[15]See U.S. General Accounting Office, *D.C. Courts: Disciplined Processes Critical to Successful System Acquisition*, GAO-02-316 (Washington, D.C.: Feb. 28, 2002), p. 10.

[16]Leading companies use a disciplined review process during prototyping to assess design maturity and stability, as well as to ensure that user requirements are addressed. Stakeholder agreements are used to document user involvement in designing and evaluating prototypes and to better ensure that products work as intended. For more information, see U.S. General Accounting Office, *Best Practices: Capturing Design and Manufacturing Knowledge Early Improves Acquisition Outcomes*, GAO-02-701 (Washington, D.C.: July 15, 2002).

limited role in the gateway project by completing risk assessments and identifying technical approaches to authentication for their individual projects; they have not been involved in determining the technologies to be incorporated in the gateway. Although the gateway is intended to deliver common, interoperable authentication services in support of the other e-government initiatives, it will be difficult to develop and operate such a system until user requirements are better defined.

Identifying authentication requirements for the other 24 e-government initiatives has been slow because deployment phases for the projects vary widely, and many are still in their early phases—making it difficult to define robust information assurance and authentication requirements. In May 2002, GSA and the Software Engineering Institute established a joint project to develop and apply a risk-based process to identify the authentication requirements for transactions associated with the other 24 e-government initiatives. Project objectives were to (1) document and characterize the transactions and data associated with each of the e-government initiatives; (2) identify the risks associated with conducting these transactions and authenticating users involved in them; (3) define associated authentication requirements; and (4) analyze the identified authentication requirements in aggregate to help define standard levels of authentication for the gateway. The result of this project was the development of a standardized e-Authentication requirements and risk analysis (e-RA) process. Subsequently, the Software Engineering Institute developed a self-directed tool, based on the e-RA process, for the agency officials to use in assessing the requirements of their own initiatives.

Because authentication requirements have been identified through the e-RA process for only 12 of the e-government initiatives (as of August 2003), the gateway risks not being able to address the wider authentication requirements that may be identified in the future for the other e-government initiatives. After participating in pilot risk assessments for four of the initiatives, the Software Engineering Institute reported that the transactions assessed in these pilot efforts were not representative of other e-government initiatives, and that no conclusion could be drawn about the extent to which the identified authentication requirements were representative of the other e-government initiatives. Altogether, as of August 2003, risk assessments had been completed for 12 e-government initiatives, including the 4 pilot risk assessments that the Software Engineering Institute participated in conducting. However, the results of these assessments were not used as input into the design of the prototype and interim gateways, and they have not been used to establish functional

requirements for the gateway. Despite the Software Engineering Institute's conclusion to the contrary, project officials said they believed the results of the four pilot risk assessments validated the assurance levels proposed by OMB and thus were sufficient as the basis for designing the gateway. GSA project officials further stated that the risk assessments were to be used to identify assurance levels for transactions, not functional requirements for the gateway. Officials indicated that functional requirements have not yet been identified, though the gateway achieved initial operating capability in June 2003.

Commercial Authentication Products Generally Are Not Interoperable

Agencies generally use commercial off-the-shelf products to implement authentication for their individual applications, and many of these products are based on unique proprietary approaches, making it difficult for them to interoperate. In January 2003, GSA analyzed data that it received from over 50 vendors in response to the RFI it issued in 2002. Vendors indicated that a wide variety of standards and protocols were being used to design and develop authentication products and services, including the Security Assertions Markup Language, the Simple Object Access Protocol, the Secure Sockets Layer protocol, the X.509 digital certificates standard, the Lightweight Directory Access Protocol, and others. Because so many different and incompatible approaches had been used to design authentication products and services, GSA officials stated that, at that time, they were unable to identify a single standard or small number of standards that would be suitable for the gateway, which must interoperate with many agency systems.

Many vendors suggested that the government develop a common methodology to link divergent applications and authentication products to the gateway. One approach to doing this would be to develop an application-programming interface (API) based on open, nonproprietary standards that would serve to connect agency applications to gateway services. Using a standard API to connect applications to use the gateway could eliminate the need to define unique interfaces for each application, and reduce development costs and implementation time frames. However, a common methodology or API to link authentication products and applications to the gateway would likely take considerable time to develop—too long to meet the gateway's planned operational milestone—and would be difficult, given that the gateway's user requirements are not yet fully defined. A technical specialist working with Mitretek, the contractor GSA hired to assist in prototype development, stated that custom software interfaces would have to be developed for each

authentication product intended to interoperate with the gateway, including customized software links between agency applications, electronic credential providers, and the gateway. According to this official, a considerable amount of time likely would be needed to develop customized APIs for each of the 24 e-government initiatives. This official further noted that the gateway prototype was tailored specifically to interoperate with two authentication systems managed by the Department of Agriculture's National Finance Center and that it took several months to develop the software interfaces for these two systems. In its attempt to reduce the number of software custom interfaces needed to link e-government initiatives to the gateway, in April 2003, GSA drafted technical guidance that encourages the use of the Security Assertions Markup Language as a standard way to interface with the gateway. However, this guidance has not yet been issued.

Further, because currently available commercial authentication products are not designed to interoperate with other products across multiple systems, developing a stable and reliable system that depends on interconnecting these technologies may prove difficult. Several commercial vendors stated that the technologies needed to support single sign-on capabilities across multiple platforms, applications, and databases have not yet been developed. A Mitretek official further indicated that commercial authentication products generally are designed to combine authorization and authentication services, because most existing systems treat both functions as one. The gateway, however, is intended to provide only authentication services, leaving agency applications the responsibility to grant access authorizations based on the authentication results. To support this requirement, vendors will need to make programming changes to "turn off" authorization services in their existing products. These changes could affect product performance and reliability. According to a NIST official, the gateway is a large and challenging project that is trying to cover a broad range of applications with different assurance requirements, in an area where technologies and business models are still evolving. These factors add to the development risk and argue for an extended period of testing before the gateway is made operational.

Finally, GSA has not yet addressed how the gateway's software will interoperate with systems maintained by nongovernment organizations and individual citizens. According to a NIST official, GSA's concept for delivering gateway services to citizens is heavily dependent on the relationships established between citizens and nongovernment organizations, such as financial institutions, airlines, and

telecommunications carriers. Under this concept, nongovernment organizations will play a key role in issuing authentication credentials to customers. Integrating the gateway with systems managed by nongovernment organizations as well as validating credentials provided to customers will be challenging, according to this NIST official. GSA officials agreed that it would be a challenge to establish relationships with nongovernment credential service providers and to ensure that credentials are issued and correctly validated. GSA is attempting to establish a consortium of industry and government ECPs to promote information sharing and develop a "trust list" to facilitate the exchange of credentials across organizations. In addition, the consortium would like to adopt processes used by nongovernment organizations to issue credentials and adapt those processes to validate credentials for government transactions. Officials indicated that collaborative partnerships would be needed to ensure that authentication systems and electronic credentials interoperate successfully. As of July 2003, GSA was working with the Liberty Alliance Project and other national organizations, such as the National Automated Clearing House Association, to discuss potential solutions for authentication interoperability problems.

Resource, Security, and Privacy Issues Have Not Been Fully Addressed

Addressing funding, security, and privacy issues will be critical to the deployment of the e-Authentication gateway and to maintaining public confidence in the government's ability to provide on-line services. While GSA has developed general strategies to address funding, security, and privacy issues related to deployment of the gateway, certain issues remain outstanding.

In December 2001, GSA established a multiagency investment strategy for the gateway initiative that called for financial and personnel resource commitments from 14 different federal agencies, not all of which are responsible for leading e-government initiatives. The agencies were asked to contribute about $30 million (50 percent) of the nearly $60 million needed to implement and maintain the gateway through 2006. About $32 million was to be provided during 2002. In August 2002, GSA revised the funding strategy for the gateway and increased its cost projections for linking all 24 e-government initiatives to the gateway to about $73 million through 2008. Under the revised funding plan, 13 of the 14 federal agencies were expected to provide about $25 million beginning in 2003.

GSA's funding strategy for the gateway initiative has depended on contributions that have been less than expected and provided late in the

fiscal year. In May 2003, only five agencies had agreed to fund the gateway as proposed, contributing about $4.1 million of the nearly $25 million required. GSA drafted memorandums of understanding (MOU) to obtain funding and personnel resource commitments from other agencies on an annual basis, beginning in 2003, and as part of the original funding strategy. The MOUs identified gateway priorities, milestones, partner responsibilities, and the contributions expected from each agency. As of August 2003, GSA had discussed the proposed MOUs with 11 of the 14 agencies (80 percent) included in the initial funding strategy for the gateway and 2 additional agencies. GSA's project manager stated that 16 agencies are now part of the e-Authentication Steering Committee, and 13 agencies provided a total of $13.5 million to GSA for the gateway as of August 18, 2003, with another $3 million expected from another agency by the end of fiscal year 2003. However, GSA still needed to secure about $5.1 million for the gateway as of August 18, 2003. According to GSA's project manager, all 16 agencies serving on the Steering Committee pledged individual contributions of $337,000 and $393,000 for 2004 and 2005, respectively. Eight new members may also be added to the Steering Committee, and contributions from agencies may be reduced accordingly. GSA's project manager further stated that the estimated costs for completing the gateway were reduced to about $55 million through 2008 as part of the fiscal year 2004 budgeting process.

Because resources have not been ensured and were provided late in the fiscal year, the funding strategy poses significant risks for the gateway. According to GSA's project manager, difficulty in obtaining funds for the initiative has contributed to milestone delays and other problems. The project experienced a funding shortfall in 2003 and had to change the acquisition strategy for the initiative and reduce contracting support, according to the project manager. The GSA official added that the project might face similar funding shortfalls beyond 2003, and that GSA planned to charge subscription or service fees to agencies that use the gateway to cover operations and maintenance costs after 2004. However, GSA has not yet determined what these fees would be, and additional funding may be needed to operate and maintain the gateway if agencies do not use it as much as is expected, and service fees fall short of projections.

In addition, maintaining adequate security for the e-Authentication gateway may be difficult, because it is intended to connect with so many other systems. As more and more agency applications and ECPs are linked to the gateway, an effective configuration management program will be vital to maintain minimal levels of security for the system. GSA intends to adhere

to the National Information Assurance Certification and Accreditation Process, which establishes minimum national standards for certifying and accrediting national security systems. In April 2003, the interim gateway was granted authority to operate as part of the certification and accreditation process.

The gateway's use of personal information for identity verification also raises the potential for privacy issues. The E-Government Act of 2002 requires agencies to conduct privacy impact assessments for systems such as the gateway.[17] A privacy impact assessment is a process that helps departments and agencies determine whether new technologies, information systems, and initiatives meet privacy requirements. GSA officials stated that they are designing the gateway so that privacy information is not retained within the gateway itself, thus hoping to avoid the potential problems associated with having to adequately protect stored privacy information. However, such a strategy does not provide assurance that all aspects of privacy have been adequately identified and addressed—conducting a privacy impact assessment could provide a more comprehensive view. According to GSA officials, a privacy impact assessment has not yet been completed.

In addition, concerns have been raised about the privacy implications of aggregating information collected from multiple sources and the loss of personal privacy if records are shared across government. A recent National Research Council report[18] suggests that authentication systems obtain only necessary information from users and for well-defined purposes. According to the report, this information should be retained for a minimal period of time, and a clear policy should be established to articulate what entities will have access to collected data and for what defined purposes. Further, the system should be reviewed and periodically audited to ensure compliance with these policies, and individuals should have the right to check on and correct any personal information collected by the system. OMB recommends that agencies develop measures for ensuring compliance with the Privacy Act and other government security

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

[18]National Research Council of the National Academies, Committee on Authentication Technologies and Their Privacy Implications, *Who Goes There? Authentication Through the Lens of Privacy*, prepublication version (Washington, D.C.: Apr. 8, 2003).

standards.[19] Accordingly, agencies need to assess and plan for appropriate privacy measures when implementing systems, including authentication technologies.

Conclusions

Developing an e-Authentication gateway capable of supporting the authentication requirements of the OMB-sponsored e-government initiatives is important in ensuring that citizens can safely and securely conduct electronic business with the government. Developing such a system is an ambitious task, involving the interconnection of authentication technologies on a scale that has not been attempted before within government or private industry. In attempting to meet near-term milestones—such as the initial September 2003 deadline—GSA did not adequately address several important implementation objectives. For example, GSA has only partially completed its task of assisting e-government initiatives and other federal agencies in identifying their authentication requirements, and it has not yet enabled any of the e-government initiatives to interoperate with the interim gateway. Nor has it developed authentication profiles that address the needs of the other 24 e-government initiatives or made needed changes to its governmentwide PKI-related services contract. GSA's modest progress can be understood in light of the significant challenges that the agency faces in attempting to build the e-Authentication gateway. These challenges include a lack of comprehensive administrative polices and guidance, inadequately defined user requirements, a dearth of interoperable commercial authentication products, and important resource, security, and privacy issues. Without addressing these challenges, GSA runs the risk of deploying a system that does not address user needs or operate as required.

Recommendations for Executive Action

To address the issues associated with GSA's attempts to meet near-term milestones for implementing the e-Authentication gateway, we recommend that the Administrator of GSA

- revise the schedule for deploying a fully operational version of the gateway, based on realistic milestones for development of the gateway

[19]Office of Management and Budget, *Memorandum—Procedures and Guidance on Implementing the Government Paperwork Elimination Act*, M-00-10 (Washington, D.C.: Apr. 25, 2000).

using a competitively awarded contract, development of authentication profiles for each of the other 24 e-government initiatives, and completion of revisions to GSA's governmentwide PKI-related services contract.

To ensure that e-Authentication gateway implementation challenges are fully addressed, we recommend that the Administrator of GSA, in conjunction with the Director of OMB,

- ensure that a comprehensive framework of authentication policies and procedures related to gateway operations is developed and implemented, in conjunction with NIST, the CIO Council, and other federal agencies (the framework should include policies and standards for auditing agencies and nongovernment organizations that will be linked to the gateway for compliance with applicable security, privacy, and credential requirements);

- establish a process to complete risk assessments for the OMB e-government initiatives that require authentication services and define associated authentication requirements to ensure that the gateway's design can support the range of authentication technologies that will be needed by the e-government initiatives;

- define key technical interfaces to promote interoperability with commercial products and facilitate interconnection with ECPs;

- enhance the effectiveness of the gateway's funding strategy by defining specific contributions from federal agencies and obtaining their commitment to support the initiative, based on the project's implementation and maintenance schedule, which addresses costs through 2008; and

- establish and implement security and privacy policies for the gateway, based on input from stakeholders and potential users, to ensure that all privacy requirements are considered and addressed—including the development and completion of a privacy impact assessment that involves key stakeholders.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from the Administrator of GSA and from the Secretary of Commerce. Letters from these two agencies are reprinted in appendixes I and II. We also received

oral comments from staff of OMB's Office of General Counsel. GSA generally agreed with our discussion of the challenges hindering speedy deployment of the e-Authentication gateway, as well as our recommendations aimed at addressing these challenges. Regarding the agency's progress in developing the gateway, GSA requested that we include more information on recent developments. In response to this concern, we added information to the report to acknowledge these recent developments, as outlined by GSA in an attachment to its comments. OMB staff said the agency agreed with GSA's comments.

Regarding comments from NIST, officials generally agreed with the content of information and recommendations in the draft report. Officials requested that we update information on recently drafted authentication guidance. We updated this report accordingly.

Unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Ranking Minority Member, House Committee on Government Reform; to the Ranking Minority Member, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform; and to other interested congressional committees. We will also send copies to the Director of OMB and the Administrator of GSA. Copies will be made available to others upon request. In addition, this report will be available at no charge on the GAO Web site at www.gao.gov.

If you have any questions concerning this report, please call me at (202) 512-6240 or send E-mail to koontzl@gao.gov. Other major contributors to this report included Barbara Collier, John de Ferrari, Vijay D'Souza, Steven Law, and Yvonne Vigil.

Linda D. Koontz
Director, Information Management Issues

Comments from the General Services Administration

GSA Administrator

August 11, 2003

The Honorable David M. Walker
Comptroller General of the United States
The General Accounting Office
441 G Street NW., 7th Floor
Washington DC 20548

Dear Mr. Walker:

Thank you for the opportunity to respond to the General Accounting Office's (GAO) recent draft report regarding the General Services Administration's (GSA's) progress in implementing E-Authentication. In the September 2003 Draft Report entitled *Planned E-Authentication Gateway Faces Formidable Challenges*, the GAO offered a number of recommendations for the GSA Administrator and the Office of Management and Budget, in order that near-term milestones are met and that implementation challenges are fully met.

Because E-Authentication was tasked with serving all of the President's Management Agenda E-Gov initiatives, GSA considers the effort vital to the national interest. It is therefore important that the report accurately portray the progress made in the implementation as well as the challenges facing it. Continuing progress has been made so we ask that you accept recent developments for inclusion in your published report. For example, policies, frameworks, processes and procedures are under development simultaneously with system development and are at a more mature level than depicted in the draft report. We welcome GAO's recommendations to address the challenges that still lie before us.

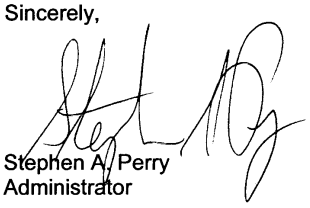
The E-Authentication effort is a complex and difficult challenge, and is at the forefront of driving technical interoperability based on emerging industry standards. Despite this complexity, the E-Authentication gateway was operational as of June 30, 2003, providing authentication services to five applications for the Social Security Administration, and it stands ready to interface to the Department of Homeland Security's Disaster Management Initiative. GSA is pleased with this progress but realizes there is still a long way to go to achieve the vision that the President's Management Council approved for this initiative.

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

Please find the enclosed GSA specific comments to the draft report findings and recommendations.

If you have any additional questions or need further assistance, please have a member of your staff contact Mary J. Mitchell, Associate Deputy Administrator, Office of Electronic Government and Technology, at (202) 501-0202.

Sincerely,



Stephen A. Perry
Administrator

Enclosure

Comments from the Department of Commerce

THE SECRETARY OF COMMERCE
Washington, D.C. 20230

August 14, 2003

Mr. Joel C. Willemssen
Managing Director, Information Technology Issues
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Willemssen:

Thank you for the opportunity to review and comment on the General Accounting Office (GAO) Draft Report GAO-03-952, *Electronic Government: Planned E-Authentication Gateway Faces Formidable Development Challenges.*

The Department of Commerce is pleased to offer comments that we believe will strengthen the report. We value the opportunity to contribute to the development of this technology and to help increase security for the Federal Government's many physical and information assets.

We look forward to your final report and will continue our efforts in support of the e-Authentication gateway throughout the Federal Government.

Sincerely,

Donald L. Evans

Enclosure

DEPARTMENT OF COMMERCE
COMMENTS ON GAO DRAFT REPORT

"Electronic Government: Planned E-Authentication Gateway Faces Formidable Development Challenges (GAO-03-952)"

We have the following comments:

1) *To ensure that e-Authentication gateway implementation challenges are fully addressed, we recommend that the Administrator of GSA, in conjunction with the Director of OMB,*

- *Ensure that a comprehensive framework of authentication policies and procedures related to gateway operation is developed and implemented, in conjunction with NIST, the CIO Council and other federal agencies. The framework should include policies for auditing agencies and nongovernment organizations that will be linked to the gateway for compliance with applicable security, privacy, and credential requirements.*

In our interview with GAO, NIST stressed the challenges of the guidance NIST is being asked to develop, and we want to reiterate that point. If a large company were implementing a corporate e-Authentication policy, they would be free to select a few specific, relatively mature authentication technologies and make their technical polices and standards specific to those specific technologies. It would be sufficient to tailor the selected approach to one solution of many. But in this effort and other security efforts NIST is constantly enjoined, often in legislation, to be technology independent, to develop performance standards and guidance that express performance requirements rather than design requirements, and that do not unduly constrain solutions, even new, immature solutions.

This is much more difficult. There is a wide range of authentication technologies available in the literature and the marketplace and it is not easy to compare and rank them all. These include:

- Symmetric key cryptography
- Public key infrastructure
- Smartcards and many other kinds of hardware identification tokens
- PINs and passwords
- Pass faces
- "Knowledge-based" authentication
- Biometrics

Each of these has many variations. It is not terribly hard to select specific variants of these technologies and develop specific technical guidance that will ensure security in

particular cases. It is much more challenging to develop technical guidance that encompasses the broad range of alternatives, and ideally accommodates future innovation. Passwords are widely used but problematic, and not well understood in some fundamental ways. On the other hand there is an urgent need to have guidance available soon. The NIST e-Authentication guidance may have to be iterative and probably developed piecemeal, with first attention given to the most widely used technologies. Any comprehensive framework of authentication policies will be evolutionary and may take some time to encompass the full range of technical possibilities. Passwords, PKI, and smartcards are the relatively common and mature technologies that we can build on first. There is a strong business case for using knowledge-based authentication, but in security terms it is much harder to evaluate, and we may have to address it in a second phase of the effort.

2) According to OMB, agencies must first identify the assurance levels associated with their planned e-government transactions and then refer to additional technical guidance to identify appropriate technical solutions. NIST has been tasked with developing this guidance, which would specify the types of technologies that could be used to conduct transactions at each of the OMB-defined assurance levels. A NIST official indicated that a working draft of this guidance likely would take several months to develop, and no specific milestone has yet been established for issuing the guidance.

NIST is working very closely and intensively with GSA in the e-Authentication effort and on a Credential Assessment Framework GSA is developing to make an initial gateway capability available in the fall of 2003. This capability will not encompass the full range of e-Authentication technologies, but will facilitate early implementation of e-Government applications. NIST expects to circulate a first draft of the overall NIST e-Authentication guidance in September 2003 for comment. Undoubtedly, both the guidance and the design of the gateway will continue to evolve for some time. This is inevitable in the rapidly evolving area of Web services and electronic service delivery.

Glossary

Authentication	The process of confirming an asserted identity with a specified or understood level of confidence.
Authorization	The granting of appropriate access privileges to authenticated users.
Application Programming Interface	An interface between the application software and the application platform (i.e., operating system), across which all services are provided.
Assurance level	In the context of authentication, the level of confidence that the relying party has that an electronic identity credential is being presented by the person whose identity is asserted by the credential.
Biometrics	Measures of an individual's unique physical characteristics or the unique ways that an individual performs an activity. Physical biometrics include fingerprints, hand geometry, facial patterns, and iris and retinal scans. Behavioral biometrics include voice patterns, written signatures, and keyboard typing techniques.
Certificate	A digital representation of information that (1) identifies the certification authority issuing it; (2) names or identifies the person, process, or equipment that is the user of the certificate; (3) contains the user's public key; (4) identifies its operational period; and (5) is digitally signed by the certification authority issuing it. A certificate is the means by which a user is linked—"bound"—to a public key.
Certification Authority	An authority trusted by one or more users to issue and manage digital certificates.
Confidentiality	The assurance that information is not disclosed to unauthorized entities or processes.

Digital signature	A special encrypted code, attached to an electronic message, that can be used to prove to a third party that the message was, in fact, signed by the originator. Digital signatures may also be attached to other electronic information and programs so that the integrity of the information and programs may be verified at a later time.
Electronic credentials	The electronic equivalent of traditional paper-based credentials—documents that vouch for an individual's identity.
Electronic credential providers	Organizations, both governmental and nongovernmental, that issue and, in some cases, maintain electronic credentials.
Electronic government	Government's use of technology, particularly Web-based applications, to enhance the access to and delivery of government information and services to citizens, business partners, employees, and other entities.
Federal Bridge Certification Authority	A system of certification authorities, directories, certificate policies, and certification practice statements designed to provide interoperability among federal agency certification authorities.
Identification	The process of determining to what identity a particular individual corresponds.
Interoperability	The ability of two or more systems or components to exchange information and to use the information that has been exchanged.
Privacy	The ability of an individual to decide when and on what terms elements of his or her personal information should be revealed.

Privacy Impact Assessment	A process that helps departments and agencies determine whether new technologies, information systems, and initiatives meet basic privacy requirements.
Public key infrastructure (PKI)	A system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances—including confidentiality, data integrity, authentication, and nonrepudiation—that are important in protecting sensitive communications and transactions.
Risk	The expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Smart card	A tamper-resistant security device—about the size of a credit card—that relies on an integrated circuit chip for information storage and processing.

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

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00