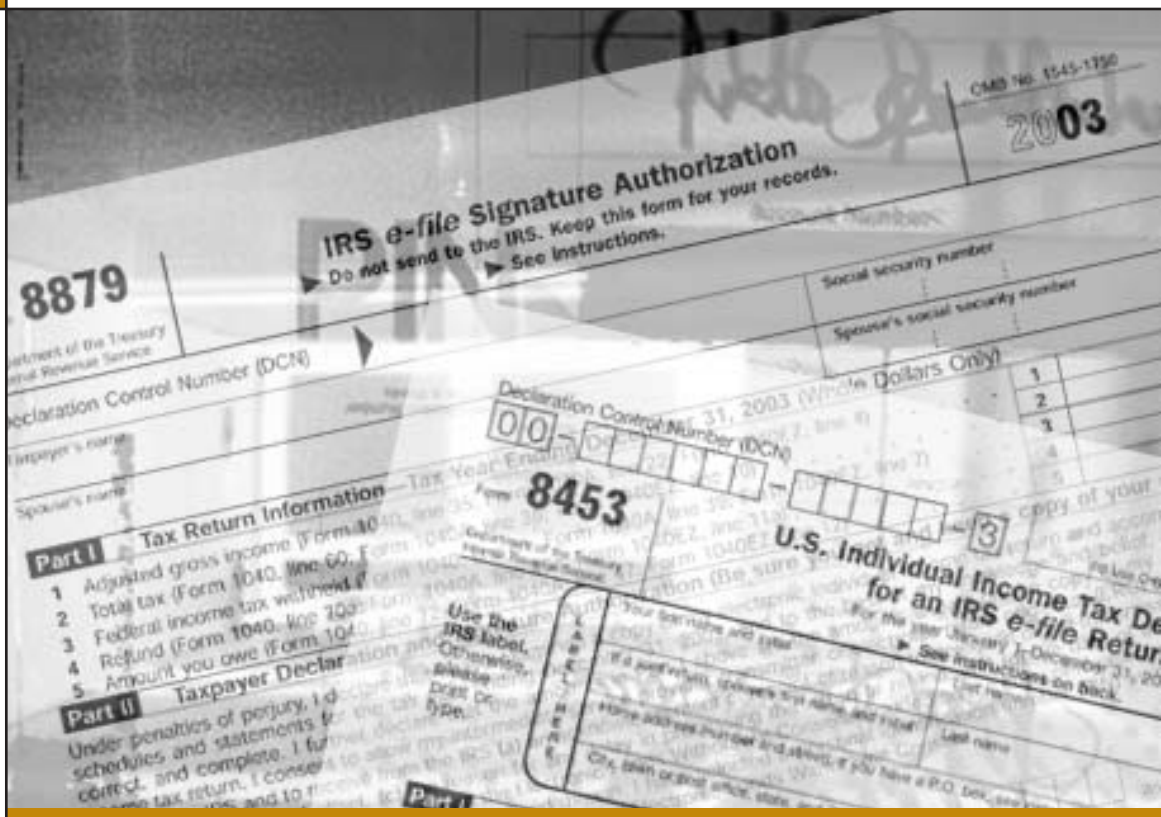
MARCH 2004

Understanding Electronic Signatures:
The Key to E-Government

E-Government Series



Stephen H. Holden
Assistant Professor of Information Systems
University of Maryland, Baltimore County

IBM Center for
The Business of Government

E-GOVERNMENT SERIES

Understanding Electronic Signatures:
The Key to E-Government

Stephen H. Holden
Assistant Professor of Information Systems
University of Maryland, Baltimore County

March 2004

TABLE OF CONTENTS

FOREWORD

March 2004

This report describes how the Internal Revenue Service (IRS) used a structured approach to assess and resolve issues and devise an innovative, practical solution for electronic signatures on electronically filed tax returns. "Understanding Electronic Signatures: The Key to E-Government" by Stephen Holden is a story of leadership and discipline. The leadership demonstrated at the IRS set the clear objective to eliminate paper in the tax filing process. The discipline employed in identifying and piloting various solutions ultimately combined the most successful aspects of each with other lessons learned to structure a successful approach.

In this report, Professor Holden highlights the importance of (1) a strategy that considers issues—policy, legal, process, technological, and stakeholder; (2) a methodical approach to piloting, learning from, and building on each potential solution; and (3) truly partnering in an arrangement where all are motivated to succeed—to the benefit not only of the public sector but also the private sector and their mutual stakeholders. Through this approach, the IRS avoided the mistakes of the past by optimizing the solution to provide for the highest stakeholder support, managing the burden, and leveraging existing technology investments. This insider's view of the history gives insight into the key decisions made by IRS leadership throughout the various phases of the evolution of their electronic signature approach.

The lessons the IRS learned from this effort are relevant to a wide range of federal agencies as they seek to address electronic authentication and make decisions about their strategies and the scope of related initiatives. While the IRS's solution is provided here not as one necessarily transferable to other agencies, the approach followed to arrive at this solution—and the insight gained into how the IRS addressed key issues and decision points—we believe to be an example useful to others pursuing the complex, critical objective of providing electronic authentication to agency constituents.

Paul Lawrence
Partner-in-Charge
IBM Center for The Business of Government
paul.lawrence@us.ibm.com

James Cook
Partner
IBM Business Consulting Services
james.e.cook@us.ibm.com

Kevin G. Belden
Associate Partner
IBM Business Consulting Services
kbelden@us.ibm.com

EXECUTIVE SUMMARY

While e-government offers many advantages to traditional service delivery, it suffers from one potentially debilitating challenge. How do users (i.e., individuals, businesses, government employees, and other stakeholders) complete transactions that by law, policy, or tradition require either a signature or some form of authentication? This report provides one possible response to the challenge of how federal agencies might eliminate paper signatures for e-government based on the experiences of one of the longest-running and arguably most successful e-government programs in the United States. The Internal Revenue Service (IRS) *e-file* program exemplifies an operational e-government program that serves tens of millions of taxpayers each year, has begun to overcome the barriers of electronic signature through several delivery channels, and has done so without relying on public key cryptography.

The IRS *e-file* program is one of the pioneers of federal e-government, dating back to the mid-1980s. Until recently, a variety of policy, management, and technology issues resulted in the IRS having to process paper signature documents for individual tax returns that were filed electronically. Despite calls from the industry groups and staff within IRS supporting *e-file* to eliminate the need for the paper signature documents due to cost and complexity concerns, the IRS was not able to craft an electronic signature solution for all facets of individual *e-file* until 1999.

Analysis of the data gathered to date indicates the IRS's use of personal identification numbers (PINs) as an electronic signature appears to have achieved several intended program results. Since the electronic signature program started, the number of returns signed electronically each year has increased. Taxpayers and preparers who used the electronic signature programs reported willingness to use the product feature in the future. Preparers achieved the goal of reducing the cost and burden of participating in the *e-file* program. Taxpayers, preparers, and the IRS all avoided the need to process paper signature forms when the return was signed and authenticated electronically. The IRS also experienced fewer paper processing costs, as a higher proportion of *e-file*d returns were totally paperless.

Even with the obvious benefits, electronic signatures clearly are not a panacea. For instance, the use of electronic signatures did not seem, in the minds of preparers, to induce taxpayers to switch from paper to electronic filing. There are still large numbers of *e-file*rs who send in paper signature documents with attachments. From the initial implementation, the IRS has changed elements of the electronic signature program to expand eligibility and ease administration for preparers and taxpayers by supplementing PINs with the use of "shared secrets" or knowledge-based authentication. Since IRS made changes to the original design of its electronic signature programs, the rate of participation by taxpayers and preparers has increased.

The IRS's use of PINs and shared secrets to sign electronic government transactions on a relatively large scale demonstrates that public organizations may be able to address what is generally reported to be a major problem facing e-government. The evolution of the IRS's electronic signature program

over the last several years has yielded lessons that are likely to be valuable as many other public organizations try to enable e-government. These lessons are particularly meaningful for those agencies that do not want to deploy public key infrastructure (PKI) solutions for electronic signatures.

Participants and observers to the electronic signature program point to a confluence of forces in late 1997 and 1998 that finally enabled the IRS to minimize if not largely eliminate paper signature documents for electronic filing of individual tax returns, which it had been talking about for more than 10 years. Legal, policy, management, leadership, and technological issues all converged within an 18- to 24-month period to make this large-scale electronic signature program successful. An analysis of the program results and summary of the interviews with participants and stakeholders provide some recommendations. The recommendations for other public-sector organizations, especially federal agencies pursuing e-government, include:

- Match the tool to the task.
- Leverage technology and the information resources you have.
- Use existing law and policy as enablers of change.
- Revise, even if at first you partially succeed.
- Establish "business ownership" of electronic signature efforts.
- Partner, partner, partner.
- Provide or obtain executive sponsorship for electronic signature efforts.

While the federal e-government strategy promotes e-authentication, primarily through PKI, as the electronic signature solution of choice for federal agencies, this report points out another answer to this e-government challenge. Given the perennial public and congressional scrutiny of the IRS, it stands to reason that other government organizations should be able to utilize some of these techniques to eliminate paper signatures in e-government programs—with taxpayers' confidence and stakeholders' acceptance.

Acknowledgments

The author wishes to thank his former colleagues at the IRS and in the tax preparation and related software industries for graciously giving their time so I could tell this story. In particular, they helped me confirm, and correct, my memory of what occurred five years ago. Special thanks to Thomas F. Baker of the IRS and Julie McEwen of the MITRE Corporation for their insightful reviews of drafts of this report. These individuals were also a vital part of my education on issues of electronic signatures and authentication when I worked at the IRS. Additionally, I want to thank Mary Ellen Corridore, who not only reviewed and commented on the manuscript, but also graciously opened her personal archives of the work we did together on this program. I could not have done this report without her good memory and great files. More important, she was the driving force behind making electronic signatures a reality for the IRS *e-file* program and one of the main reasons this is a success story. Brock Bomberger, an IS student at UMBC, provided research assistance on this report. Thanks, too, to Mark Abramson and the IBM Center staff for helping me rethink the focus of the report.

Understanding the Challenges of E-Signatures

The Rise of E-Government

Electronic government (e-government) is being touted as a solution for many of the perceived and, in some cases real, problems facing government organizations, such as lack of responsiveness, lack of efficiency, and lack of trust (Council for Excellence in Government, 2000). E-government makes it possible for public agencies to inform, serve, and interact with the public in myriad ways, generally more conveniently, often less expensively, and with higher customer satisfaction than is possible by traditional service delivery (University of Michigan, 2002).

While e-government offers many advantages to traditional service delivery, it suffers from one potentially debilitating challenge. How do users (i.e., individuals, businesses, government employees, and other stakeholders) complete transactions that by law, policy, or tradition require either a signature or some form of authentication? There are choices for program managers, but often they are characterized as technological choices. In reality, though, technology is just one part of any solution for eliminating paper signatures to enable electronic transactions. Such solutions are a mix of policy, technology, and management choices. As a result, to view the choice of an e-signature solution strictly as a technological decision holds the potential to skew the decision process.

Some public organizations are experimenting with or deploying public key infrastructures (PKIs) as a potential answer to provide electronic signatures. The federal government, in particular, through the e-authentication initiative of the e-government strategy, is encouraging agencies to rely on government-wide PKI solutions such as those offered through the General Services Administration (Forman, 2001). Other public organizations are relying on the industry practice common in e-commerce of using PINs and passwords. Within this broad category are several variations on whether the agency issues the PIN, allows the user to select a PIN, or relies on the validation of other pieces of information presented by the user to secure the transaction. On the horizon, there is the relatively new technology based on eXtensible Markup Language (XML), called Security Assertion Markup Language (SAML).

This report outlines some of these technological means of providing electronic signature solutions for federal agencies. In doing so, though, the report discusses a reality not often discussed in federal circles: There is at least one proven alternative to PKI for enabling electronic signatures. The report discusses that alternative at some length and documents the IRS's path to electronic signatures for its *e-file* program. It includes a description of the major elements of the electronic signature program and how it evolved since first being introduced in 1999. More detailed discussions of the organizational, stakeholder, and legal and policy contexts that shaped decision making for the electronic signature programs are provided in Appendix I. Based on data sources such as taxpayer and distributor surveys, program volumes, and activity-based costing, the report describes and evaluates this new e-government product feature. It also includes an analysis of interviews of IRS employees, stakeholders, and private-sector partners who either participated or watched this product feature evolve. The report concludes

with findings and recommendations for other public organizations seeking to enable electronic signatures without PKI for their e-government projects and programs based on the experiences at the IRS.

This report does not purport to be technical in nature, but nonetheless uses some technical terms and some that are unique to the IRS *e-file* program. The glossary on pages 10–11 may help readers who want basic descriptions or definitions of some of the terms used throughout the report.

The Importance of Electronic Signatures in E-Government

The need for electronic signature and authentication solutions is well documented. Models of e-government maturity assume that government agencies make the shift from just displaying information about public programs to actually enabling transactions (Hiller and Bélanger, 2001; Layne and Lee, 2001; United Nations, 2002). The completion of transactions often requires e-government users to sign or authenticate themselves since transactions generally involve the collection or disbursement of financial resources or the collection and disclosure of personally identifiable information. Congress's oversight organization, the General Accounting Office (GAO), also identifies ensuring the privacy and security of transactions to be a major challenge to federal agencies that wish to enable e-government (2000).

Some market research indicates that issues of security and privacy are quite high on the list of concerns for e-government users. Much like with e-commerce (Carton, 2002), various market research indicates the public is hesitant to exchange sensitive data with government institutions (Information Technology Association of America (ITAA), 2000; Council for Excellence in Government, 2001; Holden and Ha, 2002; Internal Revenue Service, 2002). However, research and practical experience also suggest that convenience and ease-of-use are critical acceptance factors. For these reasons, it is important to understand user attitudes, concerns, and behaviors when developing e-signature and authentication solutions.

It is equally important to map potential solutions to the specific requirements of a particular e-government application. For example, an e-government application that requires "signing" a one-time transmission from a citizen to a government agency may not require the same authentication as an e-government application that discloses confidential information back to the citizen. Understanding these distinctions can help in crafting e-signature and authentication solutions that appropriately balance security and privacy concerns with convenience and ease of use objectives.

The GPEA as a Driver of E-Government and Enabler of E-Signatures

The enactment of the Government Paperwork Elimination Act (GPEA) in 1998 provided both the impetus to use electronic authentication to support electronic transactions and the legal foundation to help make it happen. Through GPEA, Congress recognized the benefits, to both federal agencies and the public, of moving from paper-based to electronic transactions, including reduced error rates, lower processing costs, and improved customer satisfaction. As a result, GPEA required agencies by the end of fiscal year 2003 to provide for the electronic maintenance, submission, or transaction of information as a substitute for paper where practicable. The law also stipulates that agencies use and accept "electronic signatures" in this process.

The law goes so far as to define the term *electronic signature* and to legitimate the legal force of such signatures in the scope of public interactions with federal agencies. In doing so, federal law and policy help clear up what historically has been the subject of some debate among federal agencies—what is legally sufficient to "sign" a transaction with a member of the public. Section 1709(1) of the law states that the term:

> electronic signature means a method of signing an electronic message that—
> (A) identifies and authenticates a particular person as the source of the electronic message; and (B) indicates such person's approval of the information contained in the electronic message.

The law also cleared up what might have been a contentious debate in federal agency general counsel offices throughout Washington, D.C., by

addressing directly the issue of the enforceability of electronic signatures. For transactions involving electronic records submitted or maintained consistent with the policy enabled by GPEA and using electronic signatures in accordance with the same policy, neither the electronic record nor the signature is to be denied legal effect just because it is electronic instead of paper. Both Congress and the Office of Management and Budget (OMB) state that the intent is to prevent agencies or the public from reverting to paper instead of electronic transactions and signatures because of concerns that any subsequent prosecution, for instance, a benefits fraud case, might be thrown out of court.

It is important to note also that the GPEA definition of an electronic signature does not specify the technologies or policies an agency might use to comply with the law. As required by GPEA, OMB issued implementation guidance to all federal agencies. That guidance cites examples of appropriate technologies—such as PINs and passwords; digitized signatures or biometrics, such as fingerprints; and cryptographic digital signatures, such as those used in PKIs—as acceptable electronic signature solutions under GPEA. The guidance does not suggest to agencies which solution is right for any particular program area. It does, though, suggest an analytical framework for agencies to use in determining the risk inherent in the transaction they hope to automate and which authentication technology might most appropriately mitigate that risk (Office of Management and Budget, 2000).

OMB E-Authentication Guidance

Recent OMB guidance (Office of Management and Budget, 2003) on e-authentication provides further detail to federal agencies seeking to implement e-signatures consistent with GPEA. More specifically, for purposes of this report, the OMB e-authentication guidance provides up-to-date definitions of key terms in e-authentication, describes an analytical process for determining levels of risk and assurance in evaluating e-authentication solutions, and addresses the whole authentication process.

As discussed in the National Research Council report (2003) on authentication technologies and privacy implications, most discussions of authentication bog down quickly due to a lack of common understanding of fundamental terms. The OMB guidance recognized this reality and adopted many of the definitions provided by the report. In particular, the OMB guidance uses the report definition for important terms such as "authentication" and "authorization."

One of the most important contributions of the OMB guidance is to outline steps in an analytical process for assessing risks in e-government systems, categorizing those risks and then selecting a technology as part of an e-authentication solution for mitigating those risks. The risk assessment process provides for four levels of assurance for an e-government system, which then dictates different levels of assurance in the authentication solution.

In providing an overt structure and flow to analyzing and mitigating the risks of e-authentication, the OMB guidance helps remove some of the mystery from GPEA compliance. The e-authentication guidance, much like GPEA and the earlier OMB implementation guidelines for GPEA, is technology neutral, giving agencies the latitude to select the authentication solution that meets their needs. There is also a recognition that technology choices are not the only determinants for authentication solutions and that policy and business processes work together with technology to mitigate security and privacy issues in e-government.

The Federal Strategy for Electronic Government

The importance of electronic authentication was reaffirmed by the inclusion of the e-authentication initiative in the Bush administration strategic plan for e-government (Office of Management and Budget, 2002). The e-authentication project seeks to enable a form of single sign-on for users of the federal government's information and transaction web portal, http://www.firstgov.gov.

When described in terms of business goals, project plans envision a future in which firstgov.gov users would authenticate themselves once to the portal and then would be authenticated and possibly authorized for a variety of services available on the portal. Selected agencies might also accept this authentication by the portal as sufficient to fulfill electronic signature requirements for selected applications. This vision is based on belief in a user

Glossary

Adjusted Gross Income (AGI)—The number from the previous year's tax return used by the IRS as part of its knowledge-based authentication effort. Generally only the taxpayer(s), a tax preparer, and the IRS know AGI. Also, it changes each year based on taxpayers' changing circumstances, so it does not suffer the security problem of static passwords.

Certified Public Accountant (CPA)—Accountants who have taken a qualifying exam issued by state authorities. CPAs have certain privileges and responsibilities concerning representing clients before the IRS.

Council for Electronic Revenue Communication Advancement (CERCA)—The professional organization representing industry interests, such as those of software developers, financial service providers, tax preparers, and transmitters, in electronic filing.

Customer Service Number (CSN)—A five-digit personal identification number issued by the IRS for the Telefile program and contained in the Telefile packet. Taxpayers use the CSN to sign a Telefile return.

Digital Signature—A cryptographic solution to electronic signatures that relies on public key cryptography to bind a private key to the contents of a document.

***E-file* Customer Number (ECN)**—Five-digit personal identification numbers issued by the IRS (via postcard) to taxpayers who had used tax preparation software the previous year. Taxpayers used the ECNs to sign the returns.

Electronic Filing Identification Number (EFIN)—A unique identifier issued by the IRS to electronic return originators (EROs).

Electronic Return Originator (ERO)—Approved by the IRS to file returns to the IRS electronically. EROs do not necessarily prepare the returns, but they do take responsibility for transmitting returns to the IRS and complying with electronic filing regulations.

Electronic Tax Administration (ETA)—The organization in the IRS created to promote the goals of the electronic filing program.

Enrolled Agent (EA)—Tax professionals who have privileges and responsibilities similar to those of CPAs in representing clients before the IRS, but take a different qualifying exam.

eXtensible Markup Language (XML)—A very flexible data format capability that provides organizations with the ability to create, store, and exchange data in standardized ways over the Internet. It is often referred to as a "meta" data standard in that it provides descriptive data about the data contents being transmitted.

Form 8453, U.S. Individual Income Tax Declaration for an IRS *e-file* Return—The paper signature document taxpayers have to send to the IRS if they do not use electronic signatures to sign the return. Sometimes referred to as a *jurat*. (See Appendix II.)

Form 8879, IRS *e-file* Signature Authorization—The form on which taxpayers and preparers record taxpayer(s) self-selected PIN(s) and, in selected cases, authorize the preparer to enter the PIN (i.e., sign the return) on behalf of the taxpayer(s). (See Appendix III.)

Government Paperwork Elimination Act (GPEA)—The federal law defining electronic signatures for e-government transactions.

Internal Revenue Code (IRC)—The codification of federal law relating to federal tax administration. The IRC is considered to be the definitive collection of authorizing legislation for the IRS.

IRS Restructuring and Reform Act of 1998 (RRA '98)—Considered the most significant piece of legislation affecting the mission and structure of the IRS in 40 years. It contained major provisions affecting goals and incentives for the IRS *e-file* program.

Jurat—The paper signature document that taxpayers have to send to the IRS if they do not use electronic signatures to sign the return; otherwise known as form 8453.

National Association of Computerized Tax Processors (NACTP)—A professional organization that represents mostly software developers and transmitters, supporting both individual and professional tax preparation industries. NACTP works actively with the IRS on technical specifications and standards for automated return preparation.

National Association of Enrolled Agents (NAEA)—The professional organization that represents enrolled agents, which facilitated some of the early partnerships with the IRS for electronic signatures.

National Commission on Restructuring the IRS (sometimes referred to as the **Kerry/Portman Commission)**—A 17-person commission chaired by former Senator Robert Kerry and Representative Rob Portman and commissioned by Congress to examine the structure and functions of the IRS. Its analysis and recommendations served as the basis for the IRS Restructuring and Reform Act of 1998.

Online filing—The label for the channel of IRS *e-file* where taxpayers use either web-based or personal computer tax preparation software to prepare and *e-file* their return. The label is a misnomer in that all returns are transmitted through third parties and not directly to the IRS.

Personal Identification Number (PIN)—In the IRS context, five-digit numbers selected by taxpayers to sign their tax returns.

Practitioner—A general term for a broad range of private-sector tax professionals engaged in the preparation and/or filing of tax returns. In the context of this report, *practitioner* refers specifically to an electronic return originator (ERO).

Public Key Infrastructure (PKI)—A combination of technology, policy, and management that provides a variety of security services, including digital signatures, through the issuance and subsequent validation of digital credentials, often relying on "trusted third parties."

Request for Agreement (RFA)—A mechanism the IRS uses to promote competition for adding new product features to the IRS *e-file* program. The resulting agreements are not contracts because the IRS does not pay offerors. As a result, the process differs from traditional requests for proposals and is not governed by the Federal Acquisition Regulation.

Revenue Procedure—IRS policy documents that, in the case of IRS *e-file*, outline practices and procedures for businesses wishing to participate in the electronic filing program. They are not federal regulations as defined in the Administrative Procedure Act.

Revenue Protection—A program, resulting from congressional and GAO criticism of refund fraud in the electronic filing program, the IRS launched to deter and prevent refund fraud.

Security Assertion Markup Language (SAML)—An Internet standard, built on XML, which allows for systems to exchange authentication, authorization, and attribute data across organizational and system boundaries.

Taxpayer Identification Number (TIN)—The unique identifier the IRS uses to identify taxpayers' returns and related records in their information systems. This is the primary way taxpayers identify themselves to the IRS and generally is the taxpayer's Social Security number.

Telefile—A way for taxpayers who meet certain eligibility criteria to *e-file* their tax return over a Touch-Tone phone directly to the IRS through a toll-free number. The IRS eliminated paper signature documents in this electronic filing channel first.

Transmitter—Relied on by many EROs to translate output from tax preparation software into the format approved by the IRS (because the IRS does not accept electronically filed returns directly from taxpayers, except Telefile returns).

Treasury Inspector General for Tax Administration (TIGTA)—Created by the RRA '98 to serve as the inspector general for the IRS. TIGTA, however, is part of the Department of the Treasury, not the IRS.

demand to minimize the need to establish and maintain electronic authentication and signature solutions among federal agencies and programs (General Services Administration, 2002).

For most federal agencies that lack specific authorizing legislation on the issue of electronic signatures and authentication, GPEA and the resulting OMB policy constitute the most relevant public law in this policy area. It so happened in the case of the electronic signatures in *e-file* that some legislation specific to the IRS had a similar effect. The more specific legal and policy context for the IRS is discussed in more detail below, but it's worth noting that IRS-specific legislation preceded the enactment of GPEA, but only by a few months. The GPEA provisions defining an electronic signature and enforceability of those signatures were sufficiently consistent that the IRS's implementation experience can still help other federal agencies' plans for electronic signatures in the context of GPEA.

What follows is an overview of some of the technical and business choices for agencies wishing to enable electronic signatures consistent with GPEA. A more detailed discussion of how the IRS implemented electronic signatures as part of its IRS *e-file* program is presented in the next section, in part because the IRS has deployed several of the possible e-signature solutions.

Technical Approaches to Addressing the E-Signature Challenge

This brief overview of solutions to the e-signature challenge is just that: an overview. It is not intended to discuss all of the options in an exhaustive manner. Instead, the goal is to expose the reader to the major technical choices that federal managers have, understanding that an evaluation of all options would likely require a more detailed understanding and assessment of the pros and cons of each technical approach and how it maps to the agencies' business needs. In talking about these choices, O'Looney (2002) sums up the state of the practice in this area quite nicely, saying:

> Currently, there is little understanding as to what degree government leaders and administrators understand these technologies, their relative costs, or how they might best be employed in particular transaction environments. (p. 296)

This report does not purport to fill this void other than by describing and assessing PINs, as used by the IRS in its *e-file* program, as an alternative to the much more heavily touted PKI alternative.

This subsection presents two technical options that the IRS *did not* use for e-signatures. The next section addresses the IRS's approach to e-signatures as it has evolved over the last several years.

Public Key Infrastructure (PKI)

PKI is the common term used to describe a collection of management processes, policies, and technology to secure electronic transactions. The technology that distinguishes PKIs from other electronic signature solutions is public key cryptography. In public key systems, each user has two keys, and a key is essentially a very big number. One key is kept private while the other, as the name implies, is usually made public. These keys are mathematically related in a fashion so that knowledge of the public key does not allow one to determine the corresponding private key.

This property of public key cryptosystems means that data encrypted with one user's public key can be decrypted using the user's corresponding public key, without sharing the private key with others. Conversely, data transformed with a user's private key may be verified with the corresponding public key. While PKIs may provide several security services (confidentiality, document integrity, and nonrepudiation), for purposes of this document, PKI may be used to sign documents electronically through a "digital signature" (Federal PKI Steering Committee, 1998; National Research Council, 2003).

E-government systems may rely on public key systems, such as the General Services Administration's Access Certificates for E-Services (ACES) (2003), to provide what is often referred as a "digital signature." A message or document is digitally signed by transforming a summary of the document, called the message digest, using the signer's private key. The digital signature mathematically links the message digest and the user's private key, thereby linking the content of the message to the user's private key. In addition to providing an electronic signature

for the document, the digital signature protects against unauthorized modification of the document because only the corresponding public key can decrypt the message and validate the relationship between the document and the application of the private key.

It is important to note that while digital signatures may provide confidentiality of the document content, using a digital signature does not automatically encrypt the transaction. Users must also choose to use their private keys to both sign and encrypt the document content to provide both authentication and confidentiality. Digital signature technologies, though, do not operate in a vacuum and require management and policy infrastructures to provide the desired level of trust in e-government.

Most uses of public key systems require one to know that a given public key belongs to a particular person or organization. One obvious way to obtain the public key securely is to obtain it directly from the sender in a secure out-of-band channel (for example, via a personal interaction). Specifically, if a recipient knows one public key, the issuer of that public key can "vouch" for the association between a different public key and its owner by issuing a digital document of that assertion. With some additional structure, this system becomes the basis for a PKI. The entity that signs (issues) a certificate usually is referred to as a Certification Authority (CA), and it assists with the "vouching" function mentioned above.

While acknowledging the strengths of PKI as an e-signature alternative, recognizing its limitations is equally important. In the context of the IRS's e-signature and authentication requirements, PKI continues to present two primary challenges. First, the general public has not adopted PKI widely. Digital certificates and the infrastructure on which they depend can be too costly and complex for casual, occasional use. Second, the IRS business model for *e-file* includes characteristics not easily accommodated by a traditional PKI solution, including the need to file electronic returns through a third-party intermediary and to associate more than one signature (e.g., husband, wife, tax preparer) to a single return document. These limitations have led the IRS to choose, and continue to explore, alternative e-signature solutions.

Security Assertion Markup Language (SAML)

Another emerging standard holds the potential to facilitate electronic signature solutions in the future. The primary purpose of Security Assertion Markup Language (SAML) is to allow interoperability among web-based systems that supply or rely on security services by sharing information about authentication, authorization, or attributes. It is an eXtensible Markup Language (XML) framework that shares these kinds of information in the form of an assertion. For instance, SAML might facilitate an exchange of data from one federal system to another where the assertion is "user = Holden@umbc.edu." Depending on the originating system, this user might have certain characteristics and authorities associated with the user name in that domain (Organization for the Advancement of Structured Information Standards, 2003).

For purposes of this discussion, reviewing and describing SAML's common security services is worthwhile. Authentication assertions require a level of assurance on a user's identity (i.e., human or computer) (Rosencrance, 2003). For example, it is possible for a person to be a subject and identified by an e-mail address in a certain security domain. Authentication statements also report previous acts of authentication. Attribute assertions encompass specific details about the user (e.g., credit line, citizenship). An authorization assertion dictates whether or not subjects have permission to access certain resources and what specific actions a user can perform.

SAML only makes assertions about credentials; therefore, it does not authenticate or authorize users. Having said that, though, part of the appeal of SAML is its ability to facilitate single sign-ons across systems, security domains, and organizations. SAML links back to the actual authentication and makes an assertion based on the outcomes of that event. For instance, it is possible that user Holden@umbc.edu has been authenticated in the UMBC.edu domain using SAML. Other systems or organizations using SAML may, in effect, say that if the UMBC domain believes this user is Stephen H. Holden, so should they. Within a web session, users may authenticate themselves to particular domains using SAML, and subsequent domains and

systems may choose to rely on the original authentication process—thus enabling a single sign-on process.

Some business and management capabilities behind the technology allow SAML to support this functionality. SAML authorities—such as authentication authorities, attribute authorities, and policy decision points—may issue assertions. SAML provides a protocol that allows users to elicit assertions from SAML authorities and receive feedback from them about a certain subject (e.g., is this user really Steve Holden?). When a user authenticates and performs actions in a domain, the SAML authority is cognizant of past authorizations and assertions.

Valuable information from assertions and external policy stores can be used in requests to create responses for SAML authorities. Therefore, SAML authorities can be both producers and consumers of assertions, while users may only consume assertions (OASIS, 2003). With this combination of technology, business process, and policy, SAML enables trading partners to exchange authentication and authorization information, thereby supporting single sign-on that works seamlessly across sites hosted by various companies and diverse security environments (XML Magazine, 2003).

At this point, some businesses have begun to enable SAML capabilities in software and web services, but in many ways the standards-setting process is still under way. It will likely be some time before proven commercial products and services rely on SAML, which federal agencies could evaluate and consider for their e-government applications. In the meantime, this report provides some examples of e-signature capabilities in use that agencies should consider as these products and services develop and mature.

E-Signatures in the IRS *e-file* Program: A Case Study

The Government-Issued PIN (ECN)

Any discussion of e-signatures in the IRS *e-file* program has to begin with a brief mention of the historically paper-driven process for signing tax returns. In the IRS, the paper signature document historically has been called a *jurat* rather than by its official name, which is form 8453, U.S. Individual Income Tax Declaration for an IRS *e-file* Return (see Appendix II for a copy). Jurats include language that enables the IRS to pursue a criminal fraud penalty under section 7205 of the Internal Revenue Code if the taxpayer:

> Willfully makes and subscribes any return, statement, or other document, which contains or is verified by a written declaration that it is made under penalties of perjury, and which he does not believe to be true and correct....

While the Internal Revenue Code required returns to be signed, one of the stated needs was the desire of the organizations responsible for preventing and prosecuting tax fraud cases to link a taxpayer's signature to the language on the jurat that invoked criminal fraud penalties. As will be discussed, the jurat language, as much as the signature itself, needed to find life in an electronic signature solution for the IRS *e-file* program, even for simple returns like those filed through Telefile. The discussion of e-signatures using government-issued PINs begins with Telefile because this is where the IRS first began eliminating the need for jurats.

Some facets of Telefile make it a very strong test bed for eliminating the paper signature documents for a subset of the *e-file* population. The IRS "invites" taxpayers to participate in Telefile by sending a specially designed tax package through the mail to taxpayers at their address of record. The invitation process is backed by business rules that identify potential recipients based on expected eligibility (1040EZ filer, income less than $50,000, and single filer with no dependents). The package includes instructions for filing by using a Touch-Tone phone and a customer service number (CSN), which is a five-digit PIN. The IRS relies on the CSN used by the taxpayer to sign the return, but that does not authenticate the transaction since the CSN is not a unique identifier. The IRS authenticates the transaction by comparing the CSN, date of birth, taxpayer identification number (generally a Social Security number), and a name control presented by the taxpayer to those same data elements maintained in IRS databases.

Beginning in 1999, the IRS built on experience of the Telefile program to issue *e-file* customer numbers (ECNs) to individuals who had prepared their returns using web-based or personal computer tax preparation software the previous year. Taxpayers who used tax preparation software in filing season 1998, regardless of whether they filed electronically or on paper, received a postcard for the 1999 filing season with an ECN or, in the case of joint filers, two ECNs. When it came time to transmit the return to a third-party transmitter and subsequently to the IRS, the taxpayer(s) entered the ECNs issued by the IRS in order to sign the return. Similar to the use of the CSN in Telefile cited earlier, the ECN signed the return and the ECN used in conjunction with other data elements helped authenticate the

transaction. Using the ECN obviated the need for the taxpayer to submit the form 8453 to the IRS, thereby making the transaction totally paperless in most cases.

As part of the IRS's efforts to evaluate this new product offering, the Electronic Tax Administration (ETA) commissioned surveys of both users and non-users by the IRS Research organization.

Cost also turned out to be an issue to the IRS. The IRS was incurring costs for mailing the postcards with the ECNs. For the initial year of the effort, the IRS mailed postcards to approximately 12 million taxpayers related to eight million individual tax returns, with 0.7 million returns being signed electronically this way. In the second year, 2000, 1.4 million returns were e-signed with an ECN out of the 2.5 million returns *e-file*d through the online program. This was a relatively small proportion of the 11 million ECN postcards mailed, affecting 16 million individual tax returns.

The Practitioner PIN

As part of a parallel pilot, the IRS also tested an electronic signature program for taxpayers using selected preparers for the 1999 filing season, obviating the need for the preparer to mail a paper signature document. Preparers approved to participate in the pilot had their clients who were interested in paperless filing select a PIN, which was then recorded on an "IRS *e-file* Authorization Worksheet." The tax preparer kept the worksheet on file and the taxpayer got a copy. The PIN, or PINs in the case of jointly filed returns, signed the return. This solution emerged from the IRS/industry group exploring how to eliminate the paper signature document created through the request for agreement (RFA) process.

Instead of just having the preparer or taxpayer(s) retain the form 8453, the IRS/industry work group came up with a variant practice that has been implemented in several states. Based on a suggestion from an attorney from IRS chief counsel, the group fashioned a worksheet to record a PIN the taxpayer(s) would select, the preparer would record their electronic filing identification number (EFIN), and all parties would physically sign the worksheet. The taxpayer(s) used the PIN(s) to physically sign the electronic return by putting their hands on the preparer's keyboard to enter their self-selected PINs. This idea of the worksheet became what is now known as the form 8879, IRS *e-file* Signature Authorization. (See Appendix III.) That seemingly simple change to state practice garnered the sponsoring attorney a personal thank you note from the commissioner. From that point forward, the group moved from assessing feasibility to planning implementation of an idea that was a variation of what had been proposed through the RFA process. (It should be noted that having taxpayers enter their own PINs at a practitioner's keyboard proved to be a cumbersome and unpopular practice.)

Although the signature worksheet had the appearance of an 8453, there were several major differences. First, instead of having to mail the worksheet to the IRS, the tax preparation firm retained the worksheet in the taxpayers' files. Second, the worksheet recorded the PIN selected by the taxpayer(s) and entered into the preparer's computer when the return was signed. In doing so, the PIN and the signing of the return were bound to the electronic filing transaction. The worksheet became part of the return saved by the preparer, while the preparer also gave a copy to the taxpayer(s). Other than these differences, the forms 8453 and 8879 looked (and still look) quite similar because of including certain key data elements from the return.

In both the 1999 electronic signature efforts, much like with Telefile, the IRS used a PIN-like number (e.g., CSN, ECN, self-selected PIN) to sign the returns. This met the legal requirement for a return to be signed. Using the number in combination with other data presented by the taxpayer(s), the IRS was able to link the transaction to the taxpayer. The need for the subsequent authentication resulted from the use of a PIN that was not a unique identifier. Additionally, authentication beyond the signing of the return was necessary because of the business risks associated with refund fraud (called revenue protection by the IRS). Such concerns led to some additional decision rules on which preparers could participate in the initial rollout.

For the first year, both the IRS and its partners approved through the RFA process proceeded with some caution on the rollout of the preparer worksheet initiative to eliminate the need for the paper

signature documents to be mailed to the IRS. The IRS conducted the first screen from the electronic return originators (EROs) nominated by the organizations with nonmonetary agreements. The IRS approved only those EROs in "good standing" with prevailing program requirements, including whether they had a good track record of mailing in the form 8453 signature documents. Additionally, the IRS made sure the ERO had *e-file*d the previous year and had a reasonably good rate of return acceptance.

These criteria served to reward EROs that had complied with previous program requirements. This process yielded an approved list of approximately 8,000 participating EROs. The largest number of these EROs were part of a large commercial tax preparation business, and it decided to limit participation during the early stage of the filing season. As the program proved itself, in terms of both their internal business processes and the IRS response, the firm gradually increased participation at more of its locations.

The Self-Select PIN with Knowledge-Based Authentication

As already noted, several factors led the IRS to revise its electronic signature efforts from their original design in 1999. One factor contributing significantly to the desire to evolve the efforts to eliminate paper signatures was the commissioner's lack of satisfaction with the breadth and scope of the initial efforts. Former Commissioner Charles Rossotti was a major supporter of the efforts to employ electronic signatures in the IRS *e-file* program and, in initial meetings he had with ETA staff, wondered out loud why the IRS had not eliminated paper signature documents earlier. He was such a supporter, though, that he suggested that the initial pilot efforts were insufficient to eliminate paper signature documents for all *e-file*rs. In a January 2000 memo, he cited the "elimination of the paper 'jurat'" as one of five "problem areas in ETA" that prompted the creation of an IRS task force to address this issue, among others (Rossotti, 2000).

Armed with this task from the commissioner and a list of shortcomings in the PIN programs' initial design, the ETA study group addressed the major barriers to eliminating form 8453 from both the online and preparer channels. For the online channel, a primary goal was to eliminate the need to mail the ECNs. This would eliminate the costs of mailing millions of ECN postcards that ultimately were not used. Additionally, the commissioner and ETA both wanted to figure out a way to allow first-time users of either web filing or personal computer tax preparation software to avoid ever having to file a form 8453.

On the preparer side, the IRS wanted to leverage the trust relationship it had with EROs, but address the reality that EROs and taxpayers managed their relationship so that it was unlikely one taxpayer, let alone both, would physically be in the office to enter the self-selected PIN to sign the return. In both cases, there was also a desire to keep the issue of signing separate from authentication and not lose the ability to validate the authenticators presented during the transaction. What emerged was an interesting amalgam of facets of both pilots.

Online: The new solution for the online channel avoided the IRS's having to issue and mail the ECNs. Instead, it relied on the taxpayers' selecting their own five-digit PINs to sign the return. It was felt that while the self-selected PIN met the legal requirement for a signing, it did not provide sufficient risk mitigation for authentication. The team working on the commissioner's suggestions for ETA improvements recommended providing additional authentication by having taxpayers provide data from the previous year's return that generally only the taxpayer and the IRS would know. After some debate internally on how to balance the need for authentication with usability, the IRS decided to implement a self-select PIN program supplemented by having the taxpayer provide adjusted gross income and total tax from the previous year's return. The usability concern was based on a position that more than two data elements would increase the chance of the taxpayer's inadvertently entering data from the previous year's return incorrectly.

Preparer: The revisions for the preparer channel occurred in two stages. First, in 2001 the IRS took the idea of the form 8879 and added the requirement for knowledge-based authentication on the data elements of adjusted gross income and total tax. For 2002, the preparer community was able to convince the IRS that this was still not enough to

break down the barriers to paperless filing. As a result, the IRS reinstituted a form of the worksheet that did not require the knowledge-based authentication. It relied instead on the preparer to help validate claimed identity for purposes of authentication.

In response to concerns raised by preparers that their interactions with their clients may not involve a face-to-face meeting that would facilitate having the taxpayers enter their own self-selected PIN, the form 8879 became more than just a recordation of the ERO and taxpayers' signatures. The form 8879 represented an authorization for EROs to enter the PINs selected by taxpayers at the time of *e-file* transmission. This would allow, for instance, taxpayers to get completed returns from their EROs via mail and for the taxpayers to return the form 8879 with pen-and-ink signature(s) to their EROs, who then would be authorized to sign the return electronically with the PIN selected by the taxpayer. Even in the case of a face-to-face meeting when the return was transmitted, the form 8879 would allow the ERO instead of the taxpayers to enter the PIN(s) at the keyboard.

For the first year (2001), the IRS validated the adjusted gross income, total tax, and date of birth. For the online program, an incorrect date of birth resulted in the IRS rejecting the return, but EROs in the self-select PIN pilot were notified and given a chance to get the taxpayer to sign a form 8879 to fix the problem. Use of the self-select PIN was still restricted to EROs that had been approved by the IRS in 2002 (Internal Revenue Service, 2002).

The IRS further liberalized eligibility for EROs and validated one less data element on the form 8879 for the filing season in 2003. All EROs, regardless of whether they were approved by the IRS, could participate in the paperless filing program and use the form 8879. Additionally, the IRS dropped validation of total tax from the 8879 and did not reject returns outright if there was a mismatch on the date of birth (Internal Revenue Service, 2002). Table 1 summarizes the major options available to taxpayers and EROs for eliminating paper signature documents.

The IRS E-Signature Program

Volume Data

Despite variations in the efforts to eliminate paper in the IRS *e-file* program through the use of electronic signatures, it is apparent that over time the idea has gained acceptance. Table 2 provides a summary of both the absolute number of returns signed electronically and the proportion of *e-file* returns that were signed electronically (Internal Revenue Service, 2002; Treasury Inspector General for Tax Administration, 2002; Internal Revenue Service, 2003). Since all Telefile returns are signed electronically and are not the subject of this study,

Table 1: Electronic Signature Program Features by Year

Year/Filing Method	1999	2000	2001	2002	2003
Online: Government-Issued PIN (ECN)	Previous year tax prep software	Previous year tax prep software			
Online: Self-Select PIN with Knowledge-Based Authentication			Validate AGI, total tax, birth date (reject if wrong)	Validate AGI, birth date (reject if wrong)	Validate AGI, birth date (reject if wrong)
Preparer: Practitioner PIN	Selected EROs	Selected EROs		Selected EROs	All EROs
Preparer: Self-Select PIN with Knowledge-Based Authentication			Validate AGI, total tax, birth date	Validate AGI, birth date	Validate AGI, birth date

the final column highlights the impact of the electronic signature efforts exclusive of Telefile.

It's apparent from these data that the changes to the online channel to switch from ECN to self-select PIN increased participation greatly. Likewise, the reintroduction of the Practitioner PIN for 2002 boosted participation for that channel dramatically. Preliminary data from 2003 indicate that the rate of electronic signatures continues to grow as a percentage of *e-file*d returns, as shown in Table 2 (Lutes, 2003). Combined with data presented in the next section on costs, it's apparent that the IRS's electronic signature efforts have taken significant amounts of paper and related costs out of their submission processing programs (Internal Revenue Service, 2003).

Eliminating Paper Signatures as a Business Imperative

The IRS had operational reasons for eliminating paper signatures. Given the volumes of its electronic filings that included a paper signature document, the IRS *e-file* program still required a substantial amount of paper submission processing during the late 1990s. The IRS's first strategic plan for electronic tax administration, *A Strategy for Growth*, cited qualitative research that pointed to paper-based signatures for the program as inhibiting *e-file* adoption due to costs and complexity for preparers and burden for taxpayers (IRS, 2000).

The IRS *e-file* program also had quantitative market research specific to its user and distributor base that pointed to the need for an electronic signature solution to increase participation rates. The 2002 round of IRS market research of taxpayers finds that 11 percent of nonusers of *e-file* still cite concerns about lack of privacy and security as drawbacks of electronic filing. The same research also questioned tax preparers who did not participate in *e-file,* and nearly 10 percent (48 out of 500) cited the elimination of paper signature documents as an "incentive" that might change their minds about participating in the program (Internal Revenue Service, 2002).

The taskforce—led by ETA executive Jo Ann Bass and supported by the contractor who was supporting the broader organizational modernization of the IRS—helped uncover at least one reason why eliminating the paper signature documents should be higher on ETA's list of priorities. It also underscored the significant operational efficiencies associated with eliminating the form 8453 paper processing.

Based on some activity-based costing data originally gathered by the IRS, the contractor did its own analysis to examine the costs of processing electronic and paper returns. Not too surprisingly, the analysis confirmed that per-unit processing costs were lower for electronic returns than for paper returns and were decreasing as the volume of electronic filing continued to grow. At the time

Table 2: Individual IRS *e-file* and E-Signature Volumes (in Thousands)

Filing Season	Telefile	Practitioner PIN	Gov't Issued PIN (ECN)	Online: Self-Select PIN/ Knowledge-Based Authentication	Preparer: Self-Select PIN/ Knowledge-Based Authentication	Total e-sign	Total *e-file*	Percent of *e-file* with e-sign	Percent of *e-file* with e-sign (not including Telefile)
1999	5,664	500	660			6,824	29,345	23.3%	4.9%
2000	5,154	5,423	1,416			11,993	35,381	33.9%	22.6%
2001	4,411			4,222	4,678	13,311	40,244	33.1%	24.8%
2002	4,176	14,833		6,801	2,768	28,578	46,892	60.9%	57.1%
2003	4,023	21,641		8,530	2,365	36,559	52,194	70.0%	67.5%

The Impact of Electronic Filing

(*Excerpts from the* Washington Post)

The Internal Revenue Service announced yesterday that it plans a major reshuffling of its 115,000-member workforce, adding 2,200 workers to beef up its tax-enforcement arms, firing as many as 2,400 employees whose skills do not match the agency's new requirements and transferring or retraining more than 4,000 others....

The growth of electronic filing of tax returns has had a major impact on the agency's workload and is a key factor in allowing the agency to, as IRS Commissioner Mark W. Everson put it, "harvest benefits" of technology....

"When you do move to electronic filing, you no longer need to open as many envelopes, you no longer need to do as much data entry" to transfer information from a paper return to the agency's computers, Everson said in an interview....

From Albert B. Crenshaw, "IRS Reshapes Workforce: Focus on Tax Enforcement, Electronic Filing Prompts Move," the Washington Post, *January 8, 2004, page A-21.*

of the study, the analysis estimated that the average cost of processing a paper return was approximately 50 percent more per unit than for electronic. The primary difference arose from the dominant role of labor costs for processing paper returns. One surprising finding was the continued presence of direct labor costs for electronic filing, of which 85 percent was attributable to processing paper signature documents (Booz Allen Hamilton, 2000).

A Treasury Inspector General for Tax Administration (TIGTA) report examined some of these same data and reported that the paper processing for *e-file* was costing the IRS $363.73 per thousand returns based on fiscal year 2000 data. Between 2002 and 2006, TIGTA estimated, the IRS would still be spending $8.0 million annually to process paper signature documents, based on a continuation of electronic signature rates from 2001 (Treasury Inspector General for Tax Administration, 2002).

Taxpayers' Attitudes on the ECN Pilot

In 1999, the IRS surveyed a sample of taxpayers who received the ECN postcard. The North Florida District Office Research and Analysis (DORA) conducted the survey and analyzed the results for ETA, with the primary objective of assessing taxpayers' attitudes toward the ECN pilot and determining why taxpayers either did or did not use the ECN. The results of the survey were generally positive, but also found that ETA could make improvements to the ECN program to address some identified shortcomings (Internal Revenue Service North Florida DORA, 2000).

Given the ETA's stated goal of reducing the burden and complexity of IRS *e-file,* some of the survey findings illustrated that the ECN pilot represented progress against that goal. For instance, across five questions relating to satisfaction with the taxpayers' experience with the ECN, the top-two-box (e.g., satisfied, very satisfied) satisfaction was consistently over 50 percent. These questions gauged taxpayers' attitudes on whether the ECN made *e-file* more convenient and reduced the paperwork burden. More than three-quarters (78.1 percent) of taxpayers surveyed had filed using paper the previous year. On a related question, 60.2 percent said the ECN increased the likelihood of filing electronically in the future. Selected responses to an open-ended question for general comments buttressed a finding in the survey questions that those taxpayers generally had a good experience and wanted the ECN pilot to be made permanent.

These same survey results, though, also uncovered some potential design and implementation issues ETA had to consider as it moved forward. For instance, more than 32 percent of those responding said that they did not get the ECN postcard or were not sure whether they did. The DORA's research report accompanying the survey results hypothesized that taxpayers may not have realized the significance of the ECN postcard because it arrived in December and lacked the trappings of typical IRS official mail.

Also, 26.2 percent of respondents said they had used a paid preparer the previous year, meaning that they really should not have gotten an ECN postcard, based on program eligibility for users of

personal computer or web-based tax preparation software at home. More than two-thirds (64.6 percent) of the respondents said they filed on paper, representing an inconsistency with the responses cited above indicating a greater likelihood to *e-file*. Costs and security were cited as the top two reasons for not filing electronically (and therefore not using the ECN) in survey results, and responses to the open-ended question cited costs of using third-party software quite consistently.

Beyond these survey responses, the IRS was also getting correspondence in the form of e-mail to the IRS website and letters that provided further insights into frustrations for certain taxpayers. For joint filers, the issue of the IRS sending out a pair of ECNs based on the previous year's tax preparation method uncovered a problem with shifts in marital status from year to year.

A number of taxpayers wrote the IRS with conflicting concerns with the ECNs. For newly married couples, one person would have gotten the ECN but not the other; and the IRS had no ability to issue an ECN after the postcards were mailed, even for taxpayers who wanted them for signing their return electronically. In the case of spouses whose marriage was ending, the prospect of one spouse being able to file a joint return, having received the postcard with ECNs for both taxpayers, left some aggrieved spouses who recently had completed divorces feeling like they lost control of the tax-filing process.

Beyond issues of marital status, another potentially large group of taxpayers was not able to take advantage of signing returns electronically using an ECN. Filers who were new to tax preparation software for filing on the web did not get an ECN postcard since they had not prepared their return that way the previous year. Because the ECNs were issued once a year through a single data run from master file data from the previous filing season, there was no cost-effective way for taxpayers to request and be issued a PIN. This proved frustrating to taxpayers who used tax preparation software for the first time, read about the ability to sign their return electronically, and then discovered they could not because they lacked the magic postcard from the IRS with their ECN(s).

Distributors' Attitudes on E-Signatures

As part of evaluating the two electronic signature initiatives of 1999, ETA worked with the IRS Research organization to survey users of the Practitioner PIN pilot. For the pilot, the North Florida DORA conducted a survey of all 7,812 practitioners approved to participate in the 1999 launch (Internal Revenue Service North Florida DORA, 1999). The IRS received 1,062 completed surveys that provide the data for the following analysis.

As in the case of the ECN survey, the data showed that impressions of the PIN pilot were mixed. Preparers who participated in the pilot reacted positively, with more than 90 percent wanting to continue in the pilot for the upcoming year. Additionally, more than 80 percent expressed a desire for the IRS to make the PIN program permanent. Survey respondents cited multiple benefits, including increased productivity of staff, reduced paper burden, and relative ease of incorporating the PIN process into their business operations. More than 80 percent provide a top-two-box satisfaction score when asked whether the PIN was preferable to the form 8453.

Although the survey data demonstrated that the pilot addressed long-standing preparer complaints about the cost and burden of managing the form 8453s, the data also revealed some unintended consequences of the program design that presented new barriers to eliminating paper signature documents. Certain pilot program requirements—namely, that taxpayers had to physically visit their preparer's office to sign the return—created new logistical barriers for preparers.

The requirement that both taxpayers physically enter their PIN at the preparer's office ran afoul of two realities of the tax preparation business. First, the reality is that one spouse in a jointly filed return often handles most of that annual task, even if the involvement amounts to sending documents to a tax preparer and reviewing a return prepared by that third party. This means that generally only one of the taxpayers is present during the final review of the documents and signing of either the return, the signature document, or, in this case, the worksheet. Because of some nervousness about potential fraud related to electronic filing in general and

electronic signatures in particular, the IRS reemphasized the need for both taxpayers to physically sign the worksheet. This, in turn, created difficulty for preparers who had had relationships with taxpayers for years and understood that the taxpayer present at the signing marked the return for both. This long-standing practice helps explain why so many jointly filed returns bear signatures giving the appearance that the husband's and the wife's handwriting have begun to look similar after so many years of wedded bliss.

The second reality is that some taxpayers and their preparers do not see each other. Discussions with CPAs and enrolled agents revealed that some of them have been doing some clients' taxes for decades almost exclusively by exchanging paper through the mail. Once a level of comfort with this practice was established, there was no reason for the taxpayers to set foot in their tax preparer's office. The preparer could send a "ready to sign" return to the client and leave the mailing to the client. Whatever benefits might have accrued to the preparer, and to a lesser extent the taxpayer(s), from eliminating the form 8453 processes apparently could not outweigh the convenience of the "by mail" business practice, for both the preparer and the taxpayers.

The DORA report summarizing the survey findings and analysis highlighted a problem with communication about program operations and eligibility. Because this was a pilot, ETA relied heavily on the three sponsoring organizations to share information with participating preparers. The survey results indicated an uneven flow of information. Because the pilot planning ran so close to the beginning of filing season, ETA was not able to take advantage of some of the regular communication channels within the IRS to get messages to the field staff who might be trying to help a preparer or taxpayer with the program. As a result, some preparers expressed frustration that they wanted to participate, but a lack of information likely led to lower use in their practices (Internal Revenue Service North Florida DORA, 1999).

While the survey was of tax preparers, it also asked for the preparers' impressions of the taxpayers' attitudes about the PIN pilot. Even though this is a form of secondhand reporting, it is widely believed that taxpayers trust their preparers more than the IRS and may be open to preparers' influence in switching from paper to electronic filing. Despite the real and perceived benefits of eliminating the form 8453s, 75 percent of preparers responding to the survey believed that using the PINS did not increase the volume of *e-file* returns. While neither the ECN nor the Practitioner PIN is assumed to have increased the rate of electronic filing, the rapid growth of electronic signatures indicates they were at least successful in eliminating millions of pieces of paper for the IRS, its distributors, and taxpayers. (Please note that only Telefile and Online Self Select eliminate paper; Practitioner PIN and Preparer Self Select both require a paper signature document, retained by the preparer.)

Applicability to Other Federal Agencies

There is much to be learned from the IRS's experience, with its various changes and evolutions. Clearly, the IRS's approach to eliminating paper signatures has "solved" the electronic signature/authentication challenge for IRS *e-file*. In the most positive sense, the IRS has used a combination of technology, policy, and management to address a long-standing concern: eliminating millions of paper signature documents in the *e-file* program. It also enhanced the usability and marketability of the IRS *e-file* product at the same time by reducing complexity and the paperwork burden.

Some would argue that tax filing requires a stronger technical solution for electronic signatures, namely PKI. Ultimately, that is not the decision the IRS made, and it may not be the decision that others need to make—given the success of their e-signature solution—so why should they move to a solution that is unproven from a business and user perspective? Moving to the theoretically "better" technical solution of PKI could best be characterized as monumentally risky, especially on the scale of tens of millions of transactions a year.

Admittedly, the IRS e-signature solution is not a multipurpose authentication solution. For instance, one limitation is that the self-select PIN supports the transaction at hand, but has no ongoing value to support subsequent electronic transactions. With an annual filing process in which the volumes are huge, the self-selected PIN for signing and knowledge-based authentication worked well for the IRS's somewhat limited purpose. Given the costs to the IRS, the ERO community, and the public of managing the paper signature documents, though, addressing these "limited" purposes yielded significant costs, burden, and time savings for all involved.

Limited-purpose authentication has helped the IRS deliver other e-government services more efficiently as well. Most taxpayers who file electronically have overpaid their taxes and are often anxious to know the status of their refunds. In 2003, the IRS enabled an online capability to check refund status on its website by using knowledge-based authentication (i.e., the taxpayer must provide the TIN, filing status, and requested refund amount as entered on the filed return). Like many states, the IRS determined that the risk of disclosure of sensitive taxpayer information is low for this application, given that it reveals only high-level status information, such as when a tax return was received and when a refund is expected to be issued. Tax return information, refund amounts, bank account numbers, addresses, etc., are not revealed. Since taxpayers are not required to "sign" this request, no PIN or other e-signature is required. By choosing an easily administered authentication mechanism, well-suited to its limited purpose, the IRS enabled the implementation of a user-friendly, high-value e-government application with relatively low complexity and cost for authentication.

However, the nature of many citizen- and business-to-government interactions, at the IRS and other federal agencies, requires a solution that allows more frequent interactions during the year, perhaps across program lines. For agencies with these needs, a one-time-use, self-selected PIN and

knowledge-based authentication undoubtedly would not be appropriate. As an example, an agency like the Veterans Benefits Administration has users who have periodic needs for interactions and transactions across benefit programs as variable as education, disability, and home loan guarantees. Assuming that some of these interactions occur more than once a year, and that sensitive information needs to be protected, a simple self-select PIN system and knowledge-based authentication would not be sufficient. But, neither is a PKI solution required.

As the IRS moved forward to enable a wider array of electronic "account services," it increased the level of required authentication, commensurate with the risk of unauthorized disclosure of sensitive information. It also adopted a different approach to PINs and authentication to accommodate recurring interactions involving multiple programs and systems and sensitive data.

The IRS is currently rolling out a suite of electronic account services for tax professionals who are known to the IRS and who file a significant number of electronic returns annually. For this purpose, the IRS has adopted what can be called a "self-selected" PIN and password program. Users are authenticated through a registration process that includes IRS identity verification, using its own and Social Security Administration information, and the mailing of a confirmation code through the U.S. Postal Service. To gain access to e-services for the first time, the confirmation code must be used in combination with the user name, self-selected password, and self-selected PIN entered during the original registration request session. Thereafter, the user name, self-selected password, and self-selected PIN authenticate the user for recurring inquiries and transactions. The system is "self-managed" in the sense that the IRS does not issue any PINs, and users who forget their user names, passwords, or PINs must reapply and reauthenticate. The IRS is not currently planning to offer electronic account services to the general public because individuals would not likely be frequent users of such services.

For agencies that have users who wish to interact or transact across a number of program lines, the use of a self-selected PIN with knowledge-based authentication might not work as well.

As an example, an agency like the Veterans Benefits Administration has users who have periodic needs for interactions and transactions across benefit programs as variable as education, disability, and home loan guarantees. Assuming that some of these interactions occur more than once a year, self-selected PINS and knowledge-based authentication may be problematic. Without having looked explicitly at the transferability of the IRS *e-file* PIN solution to other federal agencies, it is still possible to extrapolate from that experience in identifying program features that may support or frustrate this kind of approach beyond the IRS.

Table 3 outlines a representative range of e-signature and authentication alternatives and their relative strengths and weaknesses. In implementing a broad array of electronic government initiatives over the past 17 years, including electronic filing, payments, and services, the IRS has utilized each of the alternatives to some extent, with the exception of PKI and digital certificates. This is not intended to be an exhaustive list of considerations since that was not the primary focus of this study. Nonetheless, this table should provide a starting point for agencies analyzing electronic signature and authentication solutions and contemplating the lessons learned and experiences gained in the IRS *e-file* program.

This report concludes with a set of lessons learned and recommendations for other federal agencies attempting to eliminate paper signature documents in their e-government program. Interviews with IRS employees, stakeholders, and partners helped supplement the other findings to shape the following section.

Considerations for Choosing E-Signature Solutions

Match the tool to the task.
An issue closely related to using the authorities and discretion offered by GPEA and the OMB guidance is the question of how much risk mitigation agencies need when eliminating paper signatures. There is often a presumption that only PKI solutions are sufficient to meet the government's need for signature services, authentication, confidentiality, and nonrepudiation. Many civil servants arrived at that conclusion for a couple of reasons.

Table 3: Comparative Examples of E-Signature and Authentication Alternatives

E-Signature/ Authentication Method	Strengths	Weaknesses	Issues/Comments
Knowledge-based authentication	• Ease of implementation • Ease of management • Conforms to data-minimization privacy principle	• Knowledge may not be unique • Inconvenient for users	• Sufficient for low-risk, nonfinancial, and non-sensitive inquiries • By itself, not a signature mechanism
Government-issued PIN (ECN)	• Ease of implementation	• High administrative overhead for issuing, managing, and resetting PINs and revalidating identity • Inconvenient for users • Inflexible	• Difficult to predetermine user interest • May provide simple, low-cost e-signature alternative
Self-selected, single-use PIN	• Ease of implementation • Convenience to users • Minimizes PIN administration costs	• Not appropriate for recurring transactions	• May provide simple, low-cost e-signature alternative
PKI/digital certificates	• Strong access control • Secure communication (encryption) and non-repudiation • May eventually become a best practice • Provides for life cycle management (i.e., revocation, renewal, suspension, expiration) • Generally meets the strictest statutory requirements for e-signatures	• Costly, complex, and difficult to implement and use across large, diverse customer base • Low customer adoption rate • May not provide adequate identification/ authentication for government agency purposes	• Still early in life cycle, especially in government environment • Dependent on infrastructure and customer adoption rate • May be "overkill" for some applications (e.g., not requiring encryption and non-repudiation)

For starters, the e-authentication initiative in the federal e-government strategy seems to rely extensively on PKI as the favored form of electronic credential as a way to provide a single-sign-on capability for Firstgov.gov (General Services Administration, 2002). Next, the definitions of signing and authenticating are often muddled and used interchangeably. Several sources within the IRS asserted that the IRS was able to eliminate paper signature documents because, in part, the policy and implementation drew a clear distinction between signatures (which are required by law) and authentication (which is needed to manage the risk of program fraud).

Finally, there also seems to be a presumption that all federal transactions require the whole suite of security services listed above and associated as capabilities of PKIs. Agencies, when conducting their risk assessment required by OMB, should work diligently to ensure what the transaction in question really requires. Is it imperative to have technical nonrepudiation? Are there factors in internal controls or market forces that mitigate the risks of users repudiating transactions?

The market forces at work in the IRS were significant and may exist in a variety of other federal programs. The IRS used an existing chain of trust

relationships that flowed from the IRS through the EROs to the taxpayers. The IRS maintained trust by regulating the activities of the EROs such that compliance with electronic signature and authentication requirements was necessary if EROs wanted to stay in the lucrative *e-file* market space. There was also the matter of taxpayers trusting their preparers, so that if the IRS were to offer a compelling product to the preparers, they would likely recommend it to their clients.

Leverage technology and information resources you have.
While the IRS certainly had to build some databases and the IS staff wrote some new computer programs, there was no huge new PIN or authentication database. The ETA and IS staff were able to leverage both the business rules and programming for the Telefile program to create the ECNs and support the self-select PINs. One of the criteria for the ETA's working with partners on nonmonetary agreements had to be minimizing impact on IS due to workload demands relating to Y2K. What was initially viewed as a constraint likely turned out to be a critical success factor. Not only did the IRS leverage existing IS programming, but it also built the ECN effort from many of the same business rules and practices used for the Telefile CSN effort.

This meant that some of the costs and cultural barriers that normally would hold back a new product offering were overcome. On the cost issue, the changes to IS programs, in particular, were largely incremental and did not qualify as a significant new development effort. For public organizations that tend to be risk averse, like the IRS (Bozeman, 2002), being able to cite precedent tends to smooth the way for new initiatives. The fact that Telefile had used paperless signatures for three filing seasons, with no apparent adverse impact on fraud or compliance, helped mitigate concerns that expanding electronic signatures would weaken voluntary compliance with the Internal Revenue Code.

The second version of the electronic signature program, which relied on knowledge-based authentication, demonstrates the reality that many government organizations already have quite a bit of data and information about clients and users in their data stores. Some of those data go beyond the typical name, address, and client number and include transaction history, like previous year's tax liability or adjusted gross income. The IRS successfully leveraged these "shared secrets" to bring in first time *e-file*rs to overcome the limitations of the ECN effort, which limited participation to taxpayers who had filed using the web or tax preparation software the previous filing season.

Increasingly, solutions like these are referred to as "knowledge-based authentication" in that they help identify a user to a relying party, such as a government agency. Such solutions rely on validating knowledge of pieces of data from specific transactions and offer significant advantages over otherwise static shared secrets, such as mother's maiden name. Knowledge generated by transactions, by definition, is in the possession of both the user and the government agency that executed the transaction. Leveraging such data also presents the advantage that the user does not have to disclose more identifying information to either sign or authenticate than is already present in the transaction at hand or previous transaction, thereby satisfying the common privacy principle of data minimization (National Research Council, 2003).

Considerations for Implementing E-Signatures as a Change Management Exercise

Use existing law and policy as enablers of change.
It is notable that the IRS began working on eliminating paper signatures prior to the passage of either RRA '98 or GPEA. Several interviews point to debates leading up to the passage of those bills as helping to make it easier for legal staff within the IRS to consider *how* to implement instead of questioning *whether* to implement electronic signatures as a means of eliminating paper signature documents. Beyond the language on electronic signatures in RRA '98, many interviews cited the sense of urgency created within the Department of the Treasury, the IRS, and the ETA by the 80 percent electronic filing goal as a piece of important context that made the PIN pilots possible. Rather than waiting for Congress or Treasury to tell them it was okay, the ETA and the IRS used the discretion provided by the legal and policy framework they had at the time.

Moving forward, all federal agencies have both the motivation and support for change through the passage of GPEA. The subsequent guidance from OMB also provides several benefits to agencies contemplating electronic signature and authentication programs (Office of Management and Budget, 2000; Office of Management and Budget, 2003). First, GPEA is technology neutral and does not prescribe any particular technical solutions for agencies. Further, nor does the OMB guidance on implementing GPEA. Second, the OMB guidance provides an excellent analytical framework, which coincidentally mirrored the thought process the IRS went through to assess its electronic signature options.

In particular, what the IRS did and OMB requires is that agencies assess the business risks and benefits of moving from paper to electronic signature and authentication. From there, agencies should map potential technical solutions to assessed risks and benefits. No program official should accept an edict that says that either public law or government-wide policy requires a particular technical solution; that's just not true.

Revise, even if at first you partially succeed.
Spurred on by Commissioner Rossotti, stakeholders' concerns, and taxpayers' complaints, ETA staff within the IRS realized that the initial design of the electronic signature efforts, while generally successful, was not consistent with the strategic needs of the organization. The IRS also did several things that underscored the need to revise the electronic signature programs.

First, they conducted market research between both parts of the user base—practitioners (who would be viewed as distributors in a private-sector context) and taxpayers who used the ECN. Second, the ETA continued to discuss the results of the initial electronic signature program designs with software developers and practitioner groups that participated in the first two years' effort. Most important to stakeholders interviewed for this project, the ETA listened to suggestions for improvements from the private sector. In order to improve on its early, albeit modest, success, the ETA had to acknowledge that some early decisions needed to be revisited and that it had miscalculated the impact of some of the program choices.

Additionally, positive responses to eliminating paper signatures brought calls to expand eligibility for EROs and also reduce some of the administrative burden. Each year, the IRS has been able to incrementally bring more EROs and their clients into the PIN programs. This has been an explicit risk management strategy on the part of the IRS to test and implement changes at the margin once the program was launched.

Several interviewees noted that the move to eliminate paper signatures had actually increased compliance rates for signing returns. In the online channel, the compliance rates for taxpayers sending in the form 8453-OL historically had been very low, and the relative simplicity of the self-select PIN has made this almost a nonissue. For the preparer channel, compliance with signature requirements has also gone up.

The implications for EROs are quite positive. Offices that have committed totally to electronic signatures no longer have to worry about running into compliance problems for not mailing in bundles of forms 8453 and risk losing their ERO status. While volume preparers would rather not have to manage any paper related to signatures, the form 8879 and related business processes were acknowledged to be a big improvement over the form 8453.

Establish "business ownership" of electronic signature efforts.
Some observers might find this counterintuitive, as electronic signatures and authentication technologies are often the province of the CIO organization. And what exactly does "business ownership" mean? In the language of CIOs, the business owners are generally the program officials who have statutory responsibility to deliver products and services to the public, whether income support, public housing, homeland security, or crop subsidies. Typically, the CIO will work with a business owner/program official to sponsor e-government investments.

Conversely, lacking business ownership, the CIO has to sponsor investments and improvements in e-government systems without the benefit of "business" side involvement or support. In the most pos-

itive sense, ownership, whether from the business or IT side of organizations, involves providing leadership in terms of resources, vision, decision making, and stakeholder management.

As this IRS example demonstrates, though, the lack of clear business ownership likely played a role in not eliminating paper signatures before 1999. Up until this time, other parts of the IRS—notably the IS, General Counsel, and Criminal Investigations organizations—"owned" the business process around signing tax returns. In this context, that meant they drove the decision making on business rules and automation support (or lack thereof). With the creation of the ETA, though, for the first time a business organization was responsible for any benefits derived from eliminating paper signature documents to the extent that it increased electronic filing volumes. As a result, the same organization (ETA) also bore the responsibility for maintaining program integrity and minimizing fraud.

In ways that were not possible for either the CIO or Chief Counsel organization, the ETA had both the authority and the responsibility to assess and manage business risk in the design of the electronic signature efforts. ETA also had well-established ties with the external stakeholders that enabled them to work in partnership across a variety of business, technological, and policy issues. As noted in one interview, the ETA's unique executive team at the time had a combination of technological industry experience, excellent IRS operational insight, and experience in government-wide information policy.

Partner, partner, partner.
Without relying, and continuing to rely, so heavily on private-sector partners to offer *e-file* to the public, the IRS could not have made such tremendous progress. While the impetus for the practitioner pilot came from the IRS asking for external help through the Request for Agreement (RFA) process, the ECN effort was conceived internally. In both cases, the IRS responded to the well-documented requests of the primary distributors of the *e-file* product: software developers and tax preparers.

The IRS needed the support of the software developers, transmitters, and preparer community to implement these value-adding features to IRS *e-file*. IRS staff interviews generally pointed to the RFA process as a major impetus for this product offering. Industry interviews rarely mentioned the RFA unless prompted. Once prompted, though, these respondents believed that the original efforts would have been prohibitively costly and burdensome if the product feature had developed through a traditional Federal Acquisition Regulation (FAR) procurement.

While the IRS and its industry partners were reshaping their relationship in general, several interviewees pointed to the work on the PIN pilots as equally important symbolically as substantively in that both sides took some risks for a common goal. Private-sector partners were putting IS development costs and their brands at risk on an untested product. Not too surprisingly, the IRS staff thought they were taking more risks than industry, and industry felt they took more risks.

It is worth noting that the ETA worked extensively with other affected parts within the IRS to eliminate the need for paper signature documents. Although including some internal and external stakeholders in the design and implementation process seemed painful and counterproductive on some days, it ultimately contributed to the success of the effort. In many ways, this was the risk the ETA staff incurred. They had to convince the rest of the IRS, strongly inclined to resist change, that both internal and external risks were mitigated sufficiently to run the pilots. On balance, both sides took a considerable, but managed, risk.

Provide or obtain executive sponsorship.
Executive sponsorship, as is almost always the case in any change management initiative, was a critical success factor. It began with a chief officer[1] assigning the ETA ownership for authentication policy. Just signing such a memo, clarifying both authority and responsibility in an organization known for shared governance on many issues, laid the groundwork for the subsequent efforts. Having a commissioner of the IRS and an assistant commissioner of the ETA, both with substantial business and technical savvy, helped provide cover for the staff who encountered a long-running preference for paper signature documents outside the ETA organization.

Interviews from all sides pointed to executive sponsorship within the IRS, and even within the Department of the Treasury, as crucial to this effort.

It was often mentioned together with the emergence of the ETA as an organization. There was broad agreement that the ETA's singular focus, as demonstrated by significant executive involvement, on enhancing *e-file* through such new product features as electronic signatures was a major difference from previous attempts to eliminate paper signatures. When eliminating paper signatures is viewed more as a change management challenge than as a technology initiative, the importance of executive sponsorship is even more evident.

Conclusion

When asked whether any one thing in particular brought about the PIN pilots in the IRS *e-file* program in 1999, most individuals demurred. The typical response was that a confluence of policy, management, leadership, market, and technological issues all seemed to have converged at just the right time. Today, some of these conditions are even more favorable for other federal agencies considering eliminating paper signatures through the use of electronic signatures.

Because of the sensitivity of the personal information filed with the IRS each year and the perennial public and congressional scrutiny of the IRS, it stands to reason that other government organizations should be able to utilize some of these techniques. It seems safe to assert that any electronic signature solution sufficient for the IRS ought to be good enough for most federal agencies enabling e-government transactions. Proponents of e-government should not reduce efforts to deploy electronic signatures to a technological issue.

As the study points out, making the transition from paper to electronic signatures is, above all, a management and leadership challenge. For readers who say that confronting such barriers in their organizations is too hard, it stands to reason that if the IRS can do it—with its size, complexity of stakeholder relationships, and general aversion to change—so can other federal agencies.

Appendix I: Context for Electronic Signatures in the IRS *e-file* Program

The main body of the report makes it clear that the IRS did not decide on a whim in 1999 to eliminate paper signature documents from the *e-file* program. Over a number of years, the IRS gathered input from taxpayers and stakeholders on the need to eliminate paper signature documents. Working with the Department of the Treasury, the IRS ensured that the legal and policy framework was in place to enable electronic signatures. Through the issuance of the CSNs for Telefile, the IRS gained valuable experience issuing PINs and using them to have taxpayers sign returns electronically. These combined experiences, along with the pent up frustration of major *e-file* stakeholders, set the stage for a major move forward in electronic signatures in 1999. The rest of this appendix provides the various contexts that contributed to a climate favorable to eliminating paper signature documents.

Historical Context

The IRS accepted nearly 52.2 million *e-file*d returns in 2003, with well over 70 percent (36.6 million) signed electronically (Internal Revenue Service, 2003; Treasury Inspector General for Tax Administration, 2003). It's worth noting, however, that neither the level of electronic filing nor the efforts to eliminate paper signatures happened overnight. Today's IRS *e-file* program grew out of a pilot project sponsored by the Planning and Research Division in 1986. The IRS exchanged tax return data electronically at three locations with selected H&R Block tax preparation outlets (Venkatraman and Kambril, 1991; Lacijan and Crockett, 2000).

From the modest pilot test in 1986, the electronic filing program gradually grew in maturity and volume. By 1990, electronic filing had proven itself sufficiently as a research pilot for the IRS to make it available nationwide. Telefile, a program to enable selected 1040EZ filers to file their returns using a Touch-Tone phone, began in 1992. Online filing, which is really a misnomer since taxpayers had to use personal computer tax preparation software, was introduced in 1994. By 1996, Telefile had evolved so that it was paperless by implementing the first electronic signature solution for individual tax filing. In 1998, the IRS's electronic filing program for individual tax returns was renamed the IRS *e-file* as part of a new effort to brand and promote the IRS's premier e-government offering. Table A.1 depicts the growth and evolution of the IRS *e-file* program by individual tax return product area.

While the IRS *e-file* program has experienced significant growth, especially in the last several years, the IRS was under significant pressure in the mid to late 1990s to more rapidly increase the proportion of returns filed electronically. Some of the pressure was internal as the IRS sought to decrease its reliance on the expensive and error-prone paper submission processing it had been using since the 1960s (Lacijan and Crockett, 2000). External stakeholder groups, most notably GAO on behalf of Congress, issued a seemingly annual report saying the IRS was not doing enough to increase electronic filing rates (General Accounting Office, 1996).

Table A.1: Individual IRS *e-file* Volumes by Product (in Thousands)

Filing Season	Third-Party	Telefile	Online	Total *e-file* Returns	Total Paper Returns	Percent Share Electronic
1986	25			25	103,030	0%
1987	78			78	107,000	0%
1988	583			583	109,700	1%
1989	1,161			1,161	112,100	1%
1990	4,204			4,204	113,700	4%
1991	7,567			7,567	114,700	7%
1992	10,919	125		11,044	113,600	10%
1993	12,334	149		12,483	114,600	11%
1994	13,502	519		14,021	115,900	12%
1995	11,126	680	1	11,807	118,200	10%
1996	11,971	2,839	158	14,968	120,400	12%
1997	14,083	4,686	367	19,136	120,332	16%
1998	17,668	5,955	942	24,565	122,967	20%
1999	21,223	5,664	2,458	29,345	125,547	23%
2000	25,201	5,161	5,019	35,381	127,474	28%
2001	28,989	4,419	6,836	40,244	129,783	31%
2002	33,288	4,176	9,428	46,892	130,625	36%
2003	36,344	4,023	11,827	52,194	131,687	40%

Sources: Internal Revenue Service, 2000; Internal Revenue Service, 2002; Internal Revenue Service, 2003.

Within the executive branch, the OMB and the Department of the Treasury were also reported to be pushing the IRS to increase electronic filing as a means of reducing paper submission processing costs. Even private-sector partners in the IRS *e-file* program, such as professional groups like the Council for Electronic Revenue Communication Enhancement (CERCA) and the National Association of Computerized Tax Processors (NACTP), argued that the IRS was still not doing enough to enable and promote electronic filing.

What many around Washington, and even around the IRS, felt was a missed opportunity to realize the benefits of electronic filing ultimately ended up being part of the rallying cry that the IRS was overdue for a major review and overhaul. Among the list of findings in public law that justified creating the National Commission on Restructuring the Internal Revenue Service, number four out of six cited the IRS's continued reliance on paper processing in the sum of 14 billion pieces of paper each tax year.

The resulting commission report (National Commission on Restructuring the Internal Revenue Service, 1997) devoted significant attention to the issue of expanding electronic filing. The resulting IRS Restructuring and Reform Act of 1998 (RRA '98), in particular, provided the IRS with several new authorities it could use to expand electronic filing. It also provided the impetus to make sure that the IRS used those authorities by instituting a target of 80 percent electronic filing by 2007 (1998).

In early 1997, while the commission was conducting hearings and gathering data, the IRS came to the understanding that it might take an organization dedicated to electronic filing to realize the expected benefits. The IRS created the Electronic Tax Administration (ETA) organization, bringing together some of the staff from around the IRS who had worked on electronic filing over the years. Previously, the electronic filing staff had been split in the Submission Processing organization, with one staff primarily working operational issues and another group reporting to an Electronic Filing executive who did outreach and stakeholder communications work.

The centralization of staff working on *e-file* issues had several effects. For the first time, electronic filing was not an issue on some other organization's "to do" list. Meeting the goals of RRA '98 and taking full advantage of the newfound authorities provided by the law were the priorities for the ETA staff. In many ways, the ETA became a primary player in the internal negotiations for resources, such as information systems programming, communications and marketing messages, and attention from general counsel for legal opinions.

With a newly chartered ETA organization, impetus and authority in public law, and an assistant commissioner with industry experience and marketing savvy in Robert E. Barr, the ETA quickly ramped up several new product features for *e-file* to increase benefits to taxpayers and preparers and reduce impediments to participation (Cohen and Eimicke, 2001). About the same time the IRS began its electronic signature efforts, it also launched new marketing and promotion efforts and created electronic payment options for both ACH debit and credit cards.

Many of these new product features grew out of a new partnership effort the IRS launched to recognize the role of tax preparers and software developers in delivering IRS *e-file* to the taxpayer. While some product features added to the IRS *e-file* program in the late 1990s could be attributed to a general climate of change at the IRS and the ETA at that time, there were specific issues and history that shaped the IRS's efforts to eliminate paper signatures.

Business Context

As the IRS *e-file* program matured, the remaining paper in this so-called electronic filing program was creating problems on several fronts. Even though electronic filing was supposed to eliminate paper processing, taxpayers or their preparers, to sign the return, had to send in the form 8453, U.S. Individual Income Tax Declaration for an IRS *e-file* Return. (See Appendix II).

These signature documents, sometimes called *jurats,* also included attachments like the W-2. This paper component of the *e-file* program meant that the IRS still had to open a piece of mail, key in some data from the form 8453, relate the signature document to the electronically filed return data, and store part of the return in a traditional paper file and another part electronically. The form 8453 required basic identifying information, such as name, address, and taxpayer identification number(s), and other data from the return, such as adjusted gross income, total tax, federal income tax withheld, and the amount of refund or balance due.

The requirement for the preparer to file the jurat with the IRS is contained in IRS Revenue Procedures governing the practices of authorized *e-file* providers, primarily the preparers and *e-file* transmitters. The procedures also require them to exercise "due diligence" in verifying the identity of taxpayers by requesting forms of identification as a means to minimize refund fraud (Internal Revenue Service, 2001). Nonetheless, internal IRS studies examining how to improve submission-processing work called for the elimination of this paper vestige of electronic filing for a number of years.

In addition to creating paperwork and processing headaches for the IRS, compliance with the paper signature requirements was burdensome for paid preparers too. The IRS *e-file* program requirements for paid preparers led them, too, to want to do away with the signature documents. IRS *e-file* procedures require that paper signature documents for returns filed electronically be sent to an IRS service center within three business days of the date when the IRS acknowledges acceptance of the return (Internal Revenue Service, 2001). As a practical matter, this policy required preparers, to take time from their other tax preparation work to bun-

dle signature documents and related attachments and send them to the IRS. Most preparers felt this was an unnecessary cost to both them and the IRS since it was widely understood that the IRS processed the return and generally paid the refund prior to receiving and processing the signature document.

This practice, while supportive of quick cycle times for refund processing, continues to be a point of contention with some enforcement offices within the IRS and the Department of the Treasury (Treasury Inspector General for Tax Administration, 2002). In reality, though, the need for the IRS to retrieve a signature document (form 8453) arises only in rare cases when suspected fraud is confirmed and the IRS and the Department of Justice pursue a possible case for prosecution.

Externally, focus group feedback from both individual taxpayers and preparers often cited the complexity of the *e-file* program as a key barrier to increased adoption. In the strategy leading up to creating the office of Electronic Tax Administration (ETA) (Internal Revenue Service, 1997), electronic authentication surfaced as an issue the IRS needed to address to increase electronic filing rates and meet both internal and external expectations.

The first formal strategy issued by the ETA organization also cited the need to address the electronic authentication issue as a strategic initiative for the organization (Internal Revenue Service, 2000). There seemed to be widespread external support but limited support within the IRS, for using electronic signatures to eliminate paper signatures, but the limited progress was not the result of any clear prohibition in public law or policy.

IRS Legal Policy Context

Fortunately for the IRS, public law and policy supported electronic signatures and authentication as a means of eliminating paper signatures. The basic requirement in the Internal Revenue Code was, and continues to be, that tax returns be signed (1954). However, the law does not specify what constitutes a signing, and, in fact, Treasury regulations give the IRS commissioner broad discretion in determining what constitutes a signing (Department of the Treasury, 1996). The IRS was able to rely on this authority and discretion to enable electronic signatures to one channel of its electronic filing program—Telefile. The operational details of electronic signing and authentication for Telefile are found earlier in this report, but the related decision making is pertinent to the legal and policy discussion at hand.

The decision to allow Telefile returns to be signed electronically was not without controversy within the IRS, but proved instructive on how the IRS later balanced what it perceived as a legal risk against other business benefits. In the case of Telefile, some offices involved in preparing tax fraud cases for prosecution by the Justice Department argued that the IRS should not risk the tax courts either declining a prosecution or overturning one for lack of a traditionally signed tax return. One of the first questions the Department of Justice asked before accepting a tax fraud case for potential prosecution was whether the IRS had a signed return to present as evidence, which in part led to this concern.

As the debate about the legal risk of accepting electronically signed returns continued for some time, an interesting fact emerged. The Justice Department, in the form of the U.S. Attorney's offices, had to set priorities for prosecutions. As a matter of practice, the Department of Justice litigated only returns that involved large amounts of fraud or large tax liabilities, neither of which was relevant in that Telefile involved 1040EZ returns. The risk of losing a tax fraud case for because it involved a Telefile return was greatly overstated since there was no history of them being prosecuted. Despite some concerns that this might set a precedent that would encourage an expansion of electronic signing, the IRS decided the business benefit of eliminating the signature documents outweighed what turned out to be minimal legal risk.

Another distinction in the Telefile solution helped pave the way for later forms of electronic signatures. The IRS went to great lengths to say that the customer service number (CSN) or PIN signed the return but did not, alone, authenticate the taxpayer. That's because the CSN was not a unique identifier. With only five characters and millions of taxpayers getting Telefile packages, some taxpayers got the same CSN. What enabled authentication of the Telefile returns was the combination of the CSN, taxpayer identification number (TIN), name control, and date of birth.

Additionally, the IRS Restructuring and Reform Act of 1998 speaks directly to the issue of electronic signatures. Prior to RRA '98, the IRS had worked for a number of years to amend the Internal Revenue Code to recognize the legal standing of electronic signatures. There was general agreement that IRS regulations provided the IRS commissioner with authority to determine what constituted a signing to fulfill the legal requirement that all tax returns be signed. Despite this regulatory flexibility, there was enough concern in Treasury and the IRS about potential litigation risks in tax court that Treasury and IRS staff worked with the IRS Restructuring Commission, and ultimately congressional staff, to include electronic signature language in the bill that became law.

As a result, RRA '98 recommended that the IRS develop procedures to accept electronic or digital signatures and also allowed the IRS to waive signature as an interim step in developing the electronic signatures procedure (Lacijan and Crockett, 2000). This waiver authority reflected the practice of many states with income taxes at the time of the commission's work and the drafting of the RRA '98 legislation, which allowed either the taxpayer or the preparer to retain a paper signature document in their records in lieu of sending it to the state tax authority.

A final piece of policy context is germane to the IRS's implementation of an electronic signature program. Soon after the formation of the ETA organization, the executive in charge of planning the electronic signature effort became convinced that too many parts of the IRS organization had asserted de facto control over the *e-file* electronic signature policy. Alternately, depending on the issue and the timing, organizational units as varied as Criminal Investigation, Research, Submission Processing, Chief Counsel, and Information Systems might weigh in on efforts to eliminate paper signature documents.

Even if these organizations did not try to assert policy control, they might be testing authentication solutions or raise objections based on policies that were open to varying interpretations. With all these organizations having legitimate interest in the issues, no one was really in charge and leading this important issue. This resulted in a lack of clarity on ownership and business orientation that likely contributed to the lack of progress in eliminating paper signature documents prior to 1998.

This changed when the chief of the Taxpayer Service organization, who reported to the commissioner and supervised the ETA, requested that his peer chief officers coordinate electronic signature efforts with the ETA. First, he asked that they provide an inventory of electronic authentication and signature efforts to ETA. Second, the memo stated that ETA would lead an effort to develop an organization-wide electronic authentication policy that would address such issues as moving to paperless authentication, using single versus multiple PINS, and establishing a framework for determining the level and type of authentication that a particular transaction might warrant. Beyond requesting support from other chief officers, the chief of Taxpayer Service requested that from that point forward (March 1997) all requests for legal opinions from chief counsel concerning authentication be coordinated through the ETA.

This final provision of the memo proved to be one of the most valuable ones. Until that time, almost anyone in the IRS who wanted to see whether their idea for eliminating paper signatures was legally acceptable could request an opinion from counsel. While several attorneys in the chief counsel specialized in this area, the Counsel organization was large and in some cases decentralized, resulting in opinions that were sometimes inconsistent. To avoid unnecessary duplication for counsel and also provide some modicum of consistency on authentication decisions, the chief counsel banded with the ETA to create a repository of authentication decisions.

This laid the groundwork for an organization-wide policy for the IRS by centralizing the decisions in one office in Chief Counsel and assigning the ETA as the business owner, so together they could rationalize the heretofore-disparate policy efforts. While the ETA was working to provide focus and energy for this issue within, it was also reaching out to its tax preparation and software preparation partners to help overcome this barrier to *e-file* adoption.

Partnership Context

What makes electronic signatures and authentication for IRS *e-file* somewhat challenging, but also

possible, is the role of intermediaries between the IRS and the taxpayer. As noted earlier in the history of the IRS *e-file* program, the IRS relies extensively on intermediaries to deliver its electronic filing products to the public. Historically, tax preparers, including commercial tax preparation services, certified public accountants and enrolled agents (EAs), file over 60 percent of individual tax returns. This holds even more so for *e-file*, where the vast majority of returns come from either tax preparers or individuals who use tax preparation software developed and sold by the private sector.

In the case of the preparers, it is worth noting that only a subset of preparers, called electronic return originators, or EROs, are authorized to *e-file* individual returns for their clients. The authorization, in this case, refers to the fact that the IRS regulates the preparers who can *e-file* in some detail. Because non-EROs may not *e-file* on behalf of their clients, incentive is strong to comply with IRS regulations and maintain access to this lucrative market. This regulatory process is part of the IRS's efforts to minimize fraud issues that have occasionally plagued the program (Internal Revenue Service, 2001).

As documented in the ETA's strategic plan, *A Strategy for Growth,* the IRS recognized that its relationship with the authorized *e-file* providers needed to change to meet the legislative targets set out in RRA '98 (Internal Revenue Service, 2000). Although not abandoning its regulatory and oversight responsibilities over the *e-file* industry, the IRS recognized that in effect it was a supplier of *e-file* products and services and that a variety of private-sector players were much like distributors to the public.

Prior to the creation of the ETA organization, the IRS and the industry had what both sides of the relationship would alternately call indifferent to stormy dealings. The recognition that such an unproductive relationship would not support the needed growth in *e-file*, and the invocation of the traditionally private-sector model of supplier/distributor relationship, enabled a relatively rapid change in the form and content of public/private partnerships in the *e-file* program. In the context of electronic signatures and authentication, the role of these third parties was crucial. The more productive partnership relationship played a role in both the planning and implementation of the electronic signature initiatives.

One of the most telling shifts in the partnership relationship between the IRS and the *e-file* industry came about through the request for agreements (RFA) the IRS released on November 27, 1998. To help provide some focus to these requests for agreements, the IRS identified several known impediments to *e-file* adoption based on informal discussions with stakeholders and distributors and other qualitative market research. The paper signature documents were one of the impediments identified in the RFA. The IRS identified the impediment in the most general terms through the RFA to not limit the range of options that respondents might put forward for consideration. Several respondents proposed solutions to eliminate the submission of paper signature documents in ways similar to solutions state tax administration organizations were using. As noted earlier, several states had started allowing electronic return originators or taxpayers to keep the signature documents.

For some proposed partnership agreements, like promoting free tax preparation and electronic filing, the IRS and an industry partner signed a nonmonetary agreement to enable a feature for the 1999 filing season. Not all of the proposed agreements were ready for such quick adoption, but the IRS did not want to dismiss the ideas out of hand. A potential outcome for an organization or organizations coming forward with a request for agreement was that the IRS would agree to work through implementing details of a proposal with selected industry partners.

In early 1998, the ETA organized a study group made up of internal and external stakeholders who had an interest in eliminating the paper signature document for taxpayers using preparers and the online filing channel. The external members included only organizations that had proposed the idea as part of RFA process, including the National Association of Enrolled Agents (NAEA), Intuit (publishers of TurboTax), and H&R Block. Members from within the IRS included staff from ETA, General Counsel, Criminal Investigation, Information Systems, Multimedia, and the Submission Processing organization. As described on page 16 in "The Practitioner PIN," this group was instrumental in eliminating the need for paper signature documents in the IRS *e-file* program for the largest group of *e-file*rs—those taxpayers who use a tax preparer.

Appendix II: IRS Form 8453

Declaration Control Number (DCN)
0 0 – – – 4

IRS Use Only—Do not write or staple in this space.

Form **8453**

Department of the Treasury
Internal Revenue Service

U.S. Individual Income Tax Declaration for an IRS *e-file* Return

For the year January 1–December 31, 2003

▶ **See instructions on back.**

OMB No. 1545-0936

2003

Use the IRS label. Otherwise, please print or type.

LABEL HERE

Your first name and initial | Last name | **Your social security number**

If a joint return, spouse's first name and initial | Last name | **Spouse's social security number**

Home address (number and street). If you have a P.O. box, see instructions. | Apt. no.

City, town or post office, state, and ZIP code

▲ **Important!** ▲
You **must** enter your SSN(s) above.

Daytime phone number
( )

Part I **Tax Return Information** (Whole dollars only)

1	Adjusted gross income (Form 1040, line 35; Form 1040A, line 22; Form 1040EZ, line 4)	1	
2	Total tax (Form 1040, line 60; Form 1040A, line 38; Form 1040EZ, line 10)	2	
3	Federal income tax withheld (Form 1040, line 61; Form 1040A, line 39; Form 1040EZ, line 7)	3	
4	Refund (Form 1040, line 70a; Form 1040A, line 45a; Form 1040EZ, line 11a)	4	
5	Amount you owe (Form 1040, line 72; Form 1040A, line 47; Form 1040EZ, line 12)	5	

Part II **Declaration of Taxpayer** (Sign only after Part I is completed.) **Be sure to keep a copy of your tax return.**

6a ☐ I consent that my refund be directly deposited as designated in the electronic portion of my 2003 Federal income tax return. If I have filed a joint return, this is an irrevocable appointment of the other spouse as an agent to receive the refund.

b ☐ I do not want direct deposit of my refund **or** I am not receiving a refund.

c ☐ I authorize the U.S. Treasury and its designated Financial Agent to initiate an ACH electronic funds withdrawal entry to the financial institution account indicated in the tax preparation software for payment of my Federal taxes owed on this return and/or a payment of estimated tax. I further understand that this authorization may apply to subsequent Federal tax payments that I direct to be debited through the Electronic Federal Tax Payment System (EFTPS). In order for me to initiate subsequent payments, I request that the IRS send me a personal identification number (PIN) to access EFTPS. This authorization is to remain in full force and effect until I notify the U.S. Treasury Financial Agent to terminate the authorization. To revoke a payment, I must contact the U.S. Treasury Financial Agent at **1-888-353-4537** no later than 2 business days prior to the payment (settlement) date. I also authorize the financial institutions involved in the processing of the electronic payment of taxes to receive confidential information necessary to answer inquiries and resolve issues related to the payment.

If I have filed a balance due return, I understand that if the IRS does not receive full and timely payment of my tax liability, I will remain liable for the tax liability and all applicable interest and penalties. If I have filed a joint Federal and state tax return and there is an error on my state return, I understand my Federal return will be rejected.

Under penalties of perjury, I declare that the information I have given my ERO and the amounts in Part I above agree with the amounts on the corresponding lines of the electronic portion of my 2003 Federal income tax return. To the best of my knowledge and belief, my return is true, correct, and complete. I consent to my ERO sending my return, this declaration, and accompanying schedules and statements to the IRS. I also consent to the IRS sending my ERO and/or transmitter an acknowledgment of receipt of transmission and an indication of whether or not my return is accepted, any indication of a refund offset, and, if rejected, the reason(s) for the rejection. If the processing of my return or refund is delayed, I authorize the IRS to disclose to my ERO and/or transmitter the reason(s) for the delay, or when the refund was sent.

Sign Here ▶ Your signature | Date ▶ Spouse's signature. If a joint return, **both** must sign. | Date

Part III **Declaration of Electronic Return Originator (ERO) and Paid Preparer** (See instructions.)

I declare that I have reviewed the above taxpayer's return and that the entries on Form 8453 are complete and correct to the best of my knowledge. If I am only a collector, I am not responsible for reviewing the return and only declare that this form accurately reflects the data on the return. The taxpayer will have signed this form before I submit the return. I will give the taxpayer a copy of all forms and information to be filed with the IRS, and have followed all other requirements in **Pub. 1345,** Handbook for Authorized IRS *e-file* Providers. If I am also the Paid Preparer, under penalties of perjury I declare that I have examined the above taxpayer's return and accompanying schedules and statements, and to the best of my knowledge and belief, they are true, correct, and complete. This Paid Preparer declaration is based on all information of which I have any knowledge.

ERO's Use Only

ERO's signature ▶ | Date | Check if also paid preparer ☐ | Check if self-employed ☐ | ERO's SSN or PTIN

Firm's name (or yours if self-employed), address, and ZIP code ▶ | EIN | Phone no. ( )

Under penalties of perjury, I declare that I have examined the above taxpayer's return and accompanying schedules and statements, and to the best of my knowledge and belief, they are true, correct, and complete. This declaration is based on all information of which I have any knowledge.

Paid Preparer's Use Only

Preparer's signature ▶ | Date | Check if self-employed ☐ | Preparer's SSN or PTIN

Firm's name (or yours if self-employed), address, and ZIP code ▶ | EIN | Phone no. ( )

For Paperwork Reduction Act Notice, see back of form. Cat. No. 62766T Form **8453** (2003)

Appendix III: IRS Form 8879

Form **8879**

Department of the Treasury
Internal Revenue Service

IRS *e-file* Signature Authorization

▶ **Do not send to the IRS. Keep this form for your records.**
▶ **See instructions.**

OMB No. 1545-1758

2003

Declaration Control Number (DCN) ▶

Taxpayer's name	**Social security number**
Spouse's name	**Spouse's social security number**

Part I **Tax Return Information—Tax Year Ending December 31, 2003** (Whole Dollars Only)

1	Adjusted gross income (Form 1040, line 35; Form 1040A, line 22; Form 1040EZ, line 4)	1	
2	Total tax (Form 1040, line 60; Form 1040A, line 38; Form 1040EZ, line 10)	2	
3	Federal income tax withheld (Form 1040, line 61; Form 1040A, line 39; Form 1040EZ, line 7)	3	
4	Refund (Form 1040, line 70a; Form 1040A, line 45a; Form 1040EZ, line 11a)	4	
5	Amount you owe (Form 1040, line 72; Form 1040A, line 47; Form 1040EZ, line 12)	5	

Part II **Taxpayer Declaration and Signature Authorization (Be sure you get and keep a copy of your return)**

Under penalties of perjury, I declare that I have examined a copy of my electronic individual income tax return and accompanying schedules and statements for the tax year ending December 31, 2003, and to the best of my knowledge and belief, it is true, correct, and complete. I further declare that the amounts in Part I above are the amounts shown on the copy of my electronic income tax return. I consent to allow my intermediate service provider, transmitter, or electronic return originator (ERO) to send my return to the IRS and to receive from the IRS **(a)** an acknowledgement of receipt or reason for rejection of the transmission, **(b)** an indication of any refund offset, **(c)** the reason for any delay in processing the return or refund, and **(d)** the date of any refund. If applicable, I acknowledge that I have read the Electronic Funds Withdrawal Consent included on the copy of my electronic income tax return and I agree to the provisions contained therein. I have selected a personal identification number (PIN) as my signature for my electronic income tax return and, if applicable, my Electronic Funds Withdrawal Consent.

Taxpayer's PIN: check one box only

☐ I authorize ______________________ (**ERO firm name**) to enter my PIN ☐☐☐☐☐ (**do not enter all zeros**) as my signature on my tax year 2003 electronically filed income tax return.

☐ I will enter my PIN as my signature on my tax year 2003 electronically filed income tax return. Check this box **only** if you are entering your own PIN **and** your return is filed using the Practitioner PIN method. The ERO must complete Part III below.

Your signature ▶ ______________________ Date ▶ ______________

Spouse's PIN: check one box only

☐ I authorize ______________________ (**ERO firm name**) to enter my PIN ☐☐☐☐☐ (**do not enter all zeros**) as my signature on my tax year 2003 electronically filed income tax return.

☐ I will enter my PIN as my signature on my tax year 2003 electronically filed income tax return. Check this box **only** if you are entering your own PIN **and** your return is filed using the Practitioner PIN method. The ERO must complete Part III below.

Spouse's signature ▶ ______________________ Date ▶ ______________

Practitioner PIN Method Returns Only—continue below

Part III **Certification and Authentication—Practitioner PIN Method Only**

ERO's EFIN/PIN. Enter your six-digit EFIN followed by your five-digit self-selected PIN. ☐☐☐☐☐☐☐☐☐☐☐ (**do not enter all zeros**)

I certify that the above numeric entry is my PIN, which is my signature for the tax year 2003 electronically filed income tax return for the taxpayer(s) indicated above. I confirm that I am submitting this return in accordance with the requirements of the Practitioner PIN method and **Publication 1345,** Handbook for Authorized *e-file* Providers.

ERO's signature ▶ ______________________ Date ▶ ______________

ERO Must Retain This Form — See Instructions
Do Not Submit This Form to the IRS Unless Requested To Do So

For Privacy Act and Paperwork Reduction Act Notice, see back of form. Cat. No. 32778X Form **8879** (2003)

Endnotes

1. At the time of the study, chief officers were responsible for the functional offices of the IRS, like taxpayer service, collection, and exam and staff offices such as information systems and finance. These individuals and their offices reported directly to the commissioner's office and were among the most senior and well-respected career executives in the IRS. Since the IRS's organizational modernization in 2000, these positions generally no longer exist in the way discussed in this report.

Bibliography

(1954). Internal Revenue Code. 26. 6061.

(1998). Government Paperwork Elimination Act. 44. 3504.

(1998). IRS Restructuring and Reform Act of 1998.

(2000). *Electronic Government: Federal Initiatives Are Evolving Rapidly But They Face Significant Challenges.* Subcommittee on Technology, Committee on Government Reform. Washington, D.C., General Accounting Office.

Booz Allen Hamilton (2000). IRS Cost of Processing Electronic Tax Returns. Washington, D.C. Internal Revenue Service.

Bozeman, B. (2002). *Government Management of Information Mega-Technology: Lessons from the Internal Revenue Service's Tax Systems Modernization.* Arlington, Va., IBM Center for The Business of Government.

Carton, S. (2002). *The Dot.Bomb Survival Guide: Surviving and Thriving in the Dot.Com Implosion.* New York, McGraw Hill.

Cohen, S. and W. Eimicke (2001). *The Use of the Internet in Government Service Delivery.* Arlington, Va., IBM Center for The Business of Government.

Council for Excellence in Government (2000). E-Government: The Next American Revolution. 2001.

Council for Excellence in Government (2001). E-Government: The Next American Revolution. 2001.

Department of the Treasury (1996). Treasury Regulation. Washington, D.C., Department of the Treasury.

Federal PKI Steering Committee (1998). Access with Trust. Washington, D.C.: Office of Management and Budget.

Forman, Mark (2001). The Value of PKI in Achieving the Vision of E-Government. http://www.estrategy.gov/presentations/FormanCyberSpeech_PKI(11_29)/FormanCyberSpeech_PKI(11_29).ppt accessed October 9, 2003.

General Accounting Office (1996). Tax Administration: Electronic Filing Falls Short of Expectations. Washington, D.C., General Accounting Office.

General Services Administration (2002). E-authentication Initiative Request for Information. Washington, D.C., General Services Administration.

General Services Administration (2003). Access Certificates for E-Services (ACES). Washington, D.C., General Services Administration. http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentId=8646&contentType=GSA_BASIC accessed 10/9/2003.

Hiller, J. S. and F. Bélanger (2001). *Privacy Strategies for Electronic Government.* 2002.

Holden, S. H. and L. Ha (2002). "Do the Facts Match the Hype: Public Demand for, and Government Attitudes About, E-Government." *Public Administration Times.* 25: 3.

Information Technology Association of America (ITAA) (2000). Keeping the Faith: Government Information Security in the Internet Age. 2001.

Internal Revenue Service (1997). Critical Issues for Development of an Electronic Tax Administration Strategy: A Plan for Moving Federal Tax Administration into the Information Age. Washington, D.C., Internal Revenue Service.

Internal Revenue Service (2000). A Strategy For Growth. Washington D.C., Internal Revenue Service.

Internal Revenue Service (2001). Handbook for Authorized IRS *e-file* Providers of Individual Tax Returns. Washington, D.C., Internal Revenue Service.

Internal Revenue Service (2001). Questions and Answers for Tax Professionals. Washington, D.C., Internal Revenue Service.

Internal Revenue Service (2002). Findings from the 2002 Wave of *e-file* Taxpayer & Preparer Satisfaction Research. Washington, D.C., Internal Revenue Service.

Internal Revenue Service (2002). Individual Tax Statistics—Filing Season/TPUS. 2003.

Internal Revenue Service (2002). Questions and Answers for Tax Professionals. Washington, D.C., Internal Revenue Service.

Internal Revenue Service (2003). *IRS Sets New Tax Filing Season Records*. Internal Revenue Service. Retrieved May 30, 2003, from the World Wide Web: http://www.irs.gov/newsroom/article/0,,id=109446,00.html.

Internal Revenue Service North Florida DORA (1999). Practitioner PIN Pilot Study Research Report Project 1.12. Washington, D.C., Internal Revenue Service.

Internal Revenue Service North Florida DORA (2000). *e-file* Customer Number Pilot Survey Research Report: Project 1.11. Washington, D.C., Internal Revenue Service.

Lacijan, C. and A. Crockett (2000). "Making Electronic Filing a Value Proposition for Tax Practicitioners." *Journal of Tax Practice and Procedure* 2(2): 25-36.

Layne, K. and J. Lee (2001). "Developing Fully Functional E-government: A Four Stage Model." *Government Information Quarterly* 18(2): 122-136.

Lutes, T. (2003). Assistant Commissioner for Electronic Tax Administration. S. Holden. Washington, D.C.

National Commission on Restructuring the Internal Revenue Service (1997). A Vision for a New IRS. Washington, D.C., House of Representatives.

National Research Council (2003). *Who Goes There? Authentication Through the Lens of Privacy*. Washington, D.C., National Academy Press.

Office of Management and Budget (2000). Implementation of the Government Paperwork Elimination Act. 2002.

Office of Management and Budget (2003). *E-Authentication Guidance for Federal Agencies*. Washington, DC: Office of Management and Budget.

O'Looney, John A. (2002). *Wiring Governments: Challenges and Possibilities for Public Managers*. Westport, Conn.: Quorum Books.

Organization for the Advancement of Structured Information Standards (OASIS). (2003). XML cover pages, http://xml.coverpages.org/xml.html#overview. Accessed October 14, 2003.

Rosencrance, Linda. "SAML Secures Web Services." Accessed January 14, 2003. Available from http://www.computerworld.com/printthis/2002/0,4814,73712,00.html.

Rossotti, C. O. (2000). Problem Areas in ETA. B. Barr. Washington, D.C., Internal Revenue Service.

Treasury Inspector General for Tax Administration (2003). The Internal Revenue Service Continues to Pay Tax Refunds on *E-file*d Tax Returns Prior to Ensuring a Signature Document Is Processed. Washington, D.C., Department of the Treasury.

United Nations (2002). Benchmarking E-Government: A Global Perspective. New York, United Nations Division for Public Economics and Public Administration.

University of Michigan (2002). ASCI: Federal Government Scores, University of Michigan. 2002.

Venkatraman, N. and A. Kambril (1991). "The Check's Not in the Mail: Strategies for Electronic Integration in Tax Return Filing." *Sloan Management Review* (Winter): 33-43.

XML Magazine. (2003) "SAML Advances Single Sign-On Prospects." http://www.fawcette.com/xmlmag/2002_03/magazine/departments/marketscan/SAML. Accessed January 14, 2003.

ABOUT THE AUTHOR

Stephen H. Holden is an assistant professor in the Department of Information Systems at the University of Maryland, Baltimore County (UMBC). Holden's research, publications, and teachings leverage his substantial federal government experience in government-wide policy in information technology management and electronic government. His specific research interests include electronic government, information policy, electronic authentication policies and practices, the management of IT in the public sector, and electronic democracy. He has published in *IEEE Internet Computing, Public Performance and Management Review,* the *International Journal of Public Administration, Government Information Quarterly,* and several book chapters on public-sector information policy. Holden also recently participated in a National Academy of Science study team that examined the privacy impacts of authentication and published two books. He consults for several federal agencies in support of their e-government efforts and provides periodic commentary on the editorial page of *Government Computer News*. The MITRE Corporation and the IBM Endowment for The Business of Government have funded his research.

Prior to joining UMBC, he worked for the Internal Revenue Service (IRS), culminating a 16-year career in the federal career service. While at the IRS he served as the program executive, Electronic Tax Administration (ETA) Modernization, and also as the national director, Program Enhancements, reporting to the assistant commissioner (ETA). During this tenure in ETA in the IRS, he led efforts to enable electronic signatures, electronic payments, the *e-file* marketing campaign, and the request for agreement process. He also served on the Federal Public Key Infrastructure Steering Committee during his time at the IRS. Prior to going to the IRS, Holden worked for 10 years at the Office of Management and Budget (OMB), doing a variety of policy, management, and budget analysis work. Holden's federal civil servant career began in 1983 as a Presidential Management Intern at the Naval Sea Systems Command. He holds a Ph.D. (public administration and public affairs) from Virginia Polytechnic Institute and State University and an M.P.A. (Master of Public Administration) and a B.A. (public management) from the University of Maine.

KEY CONTACT INFORMATION

To contact the author:

Stephen H. Holden, Ph.D.
Department of Information Systems
University of Maryland, Baltimore County
1000 Hilltop Circle
Baltimore, MD 21250
(410) 455-3936
fax: (410) 455-1073

e-mail: Holden@umbc.edu

E-GOVERNMENT

Supercharging the Employment Agency: An Investigation of the Use of Information and Communication Technology to Improve the Service of State Employment Agencies (December 2000)

Anthony M. Townsend

Assessing a State's Readiness for Global Electronic Commerce: Lessons from the Ohio Experience (January 2001)

J. Pari Sabety
Steven I. Gordon

Privacy Strategies for Electronic Government (January 2001)

Janine S. Hiller
France Bélanger

Commerce Comes to Government on the Desktop: E-Commerce Applications in the Public Sector (February 2001)

Genie N. L. Stowers

The Use of the Internet in Government Service Delivery (February 2001)

Steven Cohen
William Eimicke

State Web Portals: Delivering and Financing E-Service (January 2002)

Diana Burley Gant
Jon P. Gant
Craig L. Johnson

Internet Voting: Bringing Elections to the Desktop (February 2002)

Robert S. Done

Leveraging Technology in the Service of Diplomacy: Innovation in the Department of State (March 2002)

Barry Fulton

Federal Intranet Work Sites: An Interim Assessment (June 2002)

Julianne G. Mahler
Priscilla M. Regan

The State of Federal Websites: The Pursuit of Excellence (August 2002)

Genie N. L. Stowers

State Government E-Procurement in the Information Age: Issues, Practices, and Trends (September 2002)

M. Jae Moon

Preparing for Wireless and Mobile Technologies in Government (October 2002)

Ai-Mei Chang
P. K. Kannan

Public-Sector Information Security: A Call to Action for Public-Sector CIOs (October 2002, 2nd ed.)

Don Heiman

The Auction Model: How the Public Sector Can Leverage the Power of E-Commerce Through Dynamic Pricing (November 2002, 2nd ed.)

David C. Wyld

The Promise of E-Learning in Africa: The Potential for Public-Private Partnerships (January 2003)

Norman LaRocque
Michael Latham

Digitally Integrating the Government Supply Chain: E-Procurement, E-Finance, and E-Logistics (February 2003)

Jacques S. Gansler
William Lucyshyn
Kimberly M. Ross

Using Technology to Increase Citizen Participation in Government: The Use of Models and Simulation (April 2003)

John O'Looney

Services Acquisition for America's Navy: Charting a New Course for SeaPort (June 2003)

David C. Wyld

E-Reporting: Strengthening Democratic Accountability (February 2004)

Mordecai Lee

Understanding Electronic Signatures: The Key to E-Government (March 2004)

Stephen H. Holden

Measuring the Performance of E-Government (March 2004)

Genie N. L. Stowers

FINANCIAL MANAGEMENT

Credit Scoring and Loan Scoring: Tools for Improved Management of Federal Credit Programs (July 1999)

Thomas H. Stanton

Using Activity-Based Costing to Manage More Effectively (January 2000)

Michael H. Granof
David E. Platt
Igor Vaysman

Audited Financial Statements: Getting and Sustaining "Clean" Opinions (July 2001)

Douglas A. Brook

An Introduction to Financial Risk Management in Government (August 2001)

Richard J. Buttimer, Jr.

Understanding Federal Asset Management: An Agenda for Reform (July 2003)

Thomas H. Stanton

Efficiency Counts: Developing the Capacity to Manage Costs at Air Force Materiel Command (August 2003)

Michael Barzelay
Fred Thompson

MARKET-BASED GOVERNMENT

Determining a Level Playing Field for Public-Private Competition (November 1999)

Lawrence L. Martin

Implementing State Contracts for Social Services: An Assessment of the Kansas Experience (May 2000)

Jocelyn M. Johnston
Barbara S. Romzek

A Vision of the Government as a World-Class Buyer: Major Procurement Issues for the Coming Decade (January 2002)

Jacques S. Gansler

Contracting for the 21st Century: A Partnership Model (January 2002)

Wendell C. Lawther

Franchise Funds in the Federal Government: Ending the Monopoly in Service Provision (February 2002)

John J. Callahan

Making Performance-Based Contracting Perform: What the Federal Government Can Learn from State and Local Governments (November 2002, 2nd ed.)

Lawrence L. Martin

Moving to Public-Private Partnerships: Learning from Experience around the World (February 2003)

Trefor P. Williams

IT Outsourcing: A Primer for Public Managers (February 2003)

Yu-Che Chen
James Perry

The Procurement Partnership Model: Moving to a Team-Based Approach (February 2003)

Kathryn G. Denhardt

Moving Toward Market-Based Government: The Changing Role of Government as the Provider (June 2003)

Jacques S. Gansler

Transborder Service Systems: Pathways for Innovation or Threats to Accountability? (March 2004)

Alasdair Roberts

HUMAN CAPITAL MANAGEMENT

Profiles in Excellence: Conversations with the Best of America's Career Executive Service (November 1999)

Mark W. Huddleston

Reflections on Mobility: Case Studies of Six Federal Executives (May 2000)

Michael D. Serlin

Managing Telecommuting in the Federal Government: An Interim Report (June 2000)

Gina Vega
Louis Brennan

Using Virtual Teams to Manage Complex Projects: A Case Study of the Radioactive Waste Management Project (August 2000)

Samuel M. DeMarie

A Learning-Based Approach to Leading Change (December 2000)

Barry Sugarman

Labor-Management Partnerships: A New Approach to Collaborative Management (July 2001)

Barry Rubin
Richard Rubin

Winning the Best and Brightest: Increasing the Attraction of Public Service (July 2001)

Carol Chetkovich

A Weapon in the War for Talent: Using Special Authorities to Recruit Crucial Personnel (December 2001)

Hal G. Rainey

A Changing Workforce: Understanding Diversity Programs in the Federal Government (December 2001)

Katherine C. Naff
J. Edward Kellough

Life after Civil Service Reform: The Texas, Georgia, and Florida Experiences (October 2002)

Jonathan Walters

The Defense Leadership and Management Program: Taking Career Development Seriously (December 2002)

Joseph A. Ferrara
Mark C. Rom

The Influence of Organizational Commitment on Officer Retention: A 12-Year Study of U.S. Army Officers (December 2002)

Stephanie C. Payne
Ann H. Huffman
Trueman R. Tremble, Jr.

Human Capital Reform: 21st Century Requirements for the United States Agency for International Development (March 2003)

Anthony C. E. Quainton
Amanda M. Fulmer

Modernizing Human Resource Management in the Federal Government: The IRS Model (April 2003)

James R. Thompson
Hal G. Rainey

Mediation at Work: Transforming Workplace Conflict at the United States Postal Service (October 2003)

Lisa B. Bingham

Growing Leaders for Public Service (November 2003)

Ray Blunt

MANAGING FOR PERFORMANCE AND RESULTS

Corporate Strategic Planning in Government: Lessons from the United States Air Force (November 2000)

Colin Campbell

Using Evaluation to Support Performance Management: A Guide for Federal Executives (January 2001)

Kathryn Newcomer
Mary Ann Scheirer

Managing for Outcomes: Milestone Contracting in Oklahoma (January 2001)

Peter Frumkin

The Challenge of Developing Cross-Agency Measures: A Case Study of the Office of National Drug Control Policy (August 2001)

Patrick J. Murphy
John Carnevale

The Potential of the Government Performance and Results Act as a Tool to Manage Third-Party Government (August 2001)

David G. Frederickson

Using Performance Data for Accountability: The New York City Police Department's CompStat Model of Police Management (August 2001)

Paul E. O'Connell

Moving Toward More Capable Government: A Guide to Organizational Design (June 2002)

Thomas H. Stanton

Performance Management: A "Start Where You Are, Use What You Have" Guide (October 2002)

Chris Wye

The Baltimore CitiStat Program: Performance and Accountability(May 2003)

Lenneal J. Henderson

Strategies for Using State Information: Measuring and Improving Program Performance (December 2003)

Shelley H. Metzenbaum

Linking Performance and Budgeting: Opportunities in the Federal Budget Process (January 2004, 2nd ed.)

Philip G. Joyce

How Federal Programs Use Outcome Information: Opportunities for Federal Managers (February 2004, 2nd ed.)

Harry P. Hatry
Elaine Morley
Shelli B. Rossman
Joseph S. Wholey

INNOVATION

Managing Workfare: The Case of the Work Experience Program in the New York City Parks Department (June 1999)

Steven Cohen

New Tools for Improving Government Regulation: An Assessment of Emissions Trading and Other Market-Based Regulatory Tools (October 1999)

Gary C. Bryner

Religious Organizations, Anti-Poverty Relief, and Charitable Choice: A Feasibility Study of Faith-Based Welfare Reform in Mississippi (November 1999)

John P. Bartkowski
Helen A. Regis

Business Improvement Districts and Innovative Service Delivery (November 1999)

Jerry Mitchell

An Assessment of Brownfield Redevelopment Policies: The Michigan Experience (November 1999)

Richard C. Hula

San Diego County's Innovation Program: Using Competition and a Whole Lot More to Improve Public Services (January 2000)

William B. Eimicke

Innovation in the Administration of Public Airports (March 2000)

Scott E. Tarry

Entrepreneurial Government: Bureaucrats as Businesspeople (May 2000)

Anne Laurent

Rethinking U.S. Environmental Protection Policy: Management Challenges for a New Administration (November 2000)

Dennis A. Rondinelli

The Challenge of Innovating in Government (February 2001)

Sandford Borins

Understanding Innovation: What Inspires It? What Makes It Successful? (December 2001)

Jonathan Walters

Government Management of Information Mega-Technology: Lessons from the Internal Revenue Service's Tax Systems Modernization (March 2002)

Barry Bozeman

Advancing High End Computing: Linking to National Goals (September 2003)

Juan D. Rogers
Barry Bozeman

NETWORKS, COLLABORATION, AND PARTNERSHIPS

Leveraging Networks to Meet National Goals: FEMA and the Safe Construction Networks (March 2002)

William L. Waugh, Jr.

21st-Century Government and the Challenge of Homeland Defense (June 2002)

Elaine C. Kamarck

Assessing Partnerships: New Forms of Collaboration (March 2003)

Robert Klitgaard
Gregory F. Treverton

Leveraging Networks: A Guide for Public Managers Working across Organizations (March 2003)

Robert Agranoff

Extraordinary Results on National Goals: Networks and Partnerships in the Bureau of Primary Health Care's 100%/0 Campaign (March 2003)

John Scanlon

Public-Private Strategic Partnerships: The U.S. Postal Service-Federal Express Alliance (May 2003)

Oded Shenkar

The Challenge of Coordinating "Big Science" (July 2003)

W. Henry Lambright

Communities of Practice: A New Tool for Government Managers (November 2003)

William M. Snyder
Xavier de Souza Briggs

TRANSFORMING ORGANIZATIONS

The Importance of Leadership: The Role of School Principals (September 1999)

Paul Teske
Mark Schneider

Leadership for Change: Case Studies in American Local Government (September 1999)

Robert B. Denhardt
Janet Vinzant Denhardt

Managing Decentralized Departments: The Case of the U.S. Department of Health and Human Services (October 1999)

Beryl A. Radin

Transforming Government: The Renewal and Revitalization of the Federal Emergency Management Agency (April 2000)

R. Steven Daniels
Carolyn L. Clark-Daniels

Transforming Government: Creating the New Defense Procurement System (April 2000)

Kimberly A. Harokopus

Trans-Atlantic Experiences in Health Reform: The United Kingdom's National Health Service and the United States Veterans Health Administration (May 2000)

Marilyn A. DeLuca

Transforming Government: The Revitalization of the Veterans Health Administration (June 2000)

Gary J. Young

The Challenge of Managing Across Boundaries: The Case of the Office of the Secretary in the U.S. Department of Health and Human Services (November 2000)

Beryl A. Radin

Creating a Culture of Innovation: 10 Lessons from America's Best Run City (January 2001)

Janet Vinzant Denhardt
Robert B. Denhardt

Transforming Government: Dan Goldin and the Remaking of NASA (March 2001)

W. Henry Lambright

Managing Across Boundaries: A Case Study of Dr. Helene Gayle and the AIDS Epidemic (January 2002)

Norma M. Riccucci

Managing "Big Science": A Case Study of the Human Genome Project (March 2002)

W. Henry Lambright

The Power of Frontline Workers in Transforming Government: The Upstate New York Veterans Healthcare Network (April 2003)

Timothy J. Hoff

Making Public Sector Mergers Work: Lessons Learned (August 2003)

Peter Frumkin

Efficiency Counts: Developing the Capacity to Manage Costs at Air Force Materiel Command (August 2003)

Michael Barzelay
Fred Thompson

Managing the New Multipurpose, Multidiscipline University Research Centers: Institutional Innovation in the Academic Community (November 2003)

Barry Bozeman
P. Craig Boardman

To download or order a copy of a report, visit the Center's website at: www.businessofgovernment.org

HEALTHCARE

The Power of Frontline Workers in Transforming Healthcare Organizations: The Upstate New York Veterans Healthcare Network (December 2003)

Timothy J. Hoff

IT Outsourcing: A Primer for Healthcare Managers (December 2003)

Yu-Che Chen
James Perry

BOOKS*

Collaboration: Using Networks and Partnerships
(Rowman & Littlefield Publishers, Inc., 2004)
John M. Kamensky and Thomas J. Burlin, editors

E-Government 2001
(Rowman & Littlefield Publishers, Inc., 2001)
Mark A. Abramson and Grady E. Means, editors

E-Government 2003
(Rowman & Littlefield Publishers, Inc., 2002)
Mark A. Abramson and Therese L. Morin, editors

Human Capital 2004
(Rowman & Littlefield Publishers, Inc., 2004)
Jonathan D. Breul and Nicole Willenz Gardner, editors

Human Capital 2002
(Rowman & Littlefield Publishers, Inc., 2002)
Mark A. Abramson and Nicole Willenz Gardner, editors

Innovation
(Rowman & Littlefield Publishers, Inc., 2002)
Mark A. Abramson and Ian Littman, editors

Leaders
(Rowman & Littlefield Publishers, Inc., 2002)
Mark A. Abramson and Kevin M. Bacon, editors

Managing for Results 2002
(Rowman & Littlefield Publishers, Inc., 2001)
Mark A. Abramson and John Kamensky, editors

Memos to the President: Management Advice from the Nation's Top Public Administrators
(Rowman & Littlefield Publishers, Inc., 2001)
Mark A. Abramson, editor

New Ways of Doing Business
(Rowman & Littlefield Publishers, Inc., 2003)
Mark A. Abramson and Ann M. Kieffaber, editors

The Procurement Revolution
(Rowman & Littlefield Publishers, Inc., 2003)
Mark A. Abramson and Roland S. Harris III, editors

Transforming Government Supply Chain Management
(Rowman & Littlefield Publishers, Inc., 2003)
Jacques S. Gansler and Robert E. Luby, Jr., editors

Transforming Organizations
(Rowman & Littlefield Publishers, Inc., 2001)
Mark A. Abramson and Paul R. Lawrence, editors

* Available at bookstores, online booksellers, and from the publisher (www.rowmanlittlefield.com or 800-462-6420).

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion on new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

The Center is one of the ways that IBM seeks to advance knowledge on how to improve public sector effectiveness. The IBM Center focuses on the future of the operation and management of the public sector.

About IBM Business Consulting Services

With consultants and professional staff in more than 160 countries globally, IBM Business Consulting Services is the world's largest consulting services organization. IBM Business Consulting Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build and run those solutions in a way that delivers bottom-line business value. For more information visit www.ibm.com/bcs.

For additional information, contact:
Mark A. Abramson
Executive Director
IBM Center for The Business of Government
1301 K Street, NW
Fourth Floor, West Tower
Washington, DC 20005
(202) 515-4504, fax: (202) 515-4375

e-mail: businessofgovernment@us.ibm.com
website: www.businessofgovernment.org