OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

CURRENT PRACTICES IN
ELECTRONIC RECORDS
AUTHENTICATION

February 2004 **A-04-04-24004**

MANAGEMENT ADVISORY REPORT

Mission

We improve SSA programs and operations and protect them against fraud, waste, and abuse by conducting independent and objective audits, evaluations, and investigations. We provide timely, useful, and reliable information and advice to Administration officials, the Congress, and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- **Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.**
- **Promote economy, effectiveness, and efficiency within the agency.**
- **Prevent and detect fraud, waste, and abuse in agency programs and operations.**
- **Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.**
- **Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.**

To ensure objectivity, the IG Act empowers the IG with:

- **Independence to determine what reviews to perform.**
- **Access to all information necessary for the reviews.**
- **Authority to publish findings and recommendations based on the reviews.**

Vision

By conducting independent and objective audits, investigations, and evaluations, we are agents of positive change striving for continuous improvement in the Social Security Administration's programs, operations, and management and in our own office.

SOCIAL SECURITY

MEMORANDUM

Date: February 3, 2004

To: The Commissioner

From: Inspector General

Subject: Current Practices in Electronic Records Authentication (A-04-04-24004)

OBJECTIVE

The objective of our review was to identify current practices for electronic records authentication in place at public and private entities.

BACKGROUND

On June 30, 2000, the President signed Senate Bill 761, entitled Electronic Signatures in Global and National Commerce Act (Act).[1] Under this legislation, no contract, signature or record can be denied legal effect solely because it is in an electronic form.[2] The Act does not describe how to implement electronic signatures or what technology to use.

Increasingly, Federal agencies are using the World Wide Web and other Internet-based applications to provide on-line public access to information and services, as well as to improve internal business operations. Identity fraud is forcing public and private organizations to carefully address the issue of user authentication.

Some current methods to authenticate electronic records include public key infrastructure (PKI), knowledge-based authentication, and electronic signature capture. See Appendix A for additional background information, scope and methodology.

[1] Pub. Law No. 106-229.

[2] 15 U.S.C. § 7001(a)(1)(2003).

RESULTS OF REVIEW

The Social Security Administration (SSA) continues to move forward with its electronic service delivery initiative, which will ultimately allow work to be handled electronically, in a paperless environment. Under this initiative, records will be accessed and verified electronically and customer interaction will occur through secure networks. SSA has a choice of several electronic records authentication technologies for use in its electronic service delivery initiative including PKI, knowledge-based authentication, and electronic signature capture. SSA currently uses PKI and knowledge-based authentication in some areas of its business operations.

We believe it is beneficial for SSA to consider the experiences of other public and private organizations with electronic records authentication technologies as they relate to the agency's electronic service delivery initiative. This report provides information on the experiences that some private and public entities have with PKI, knowledge-based authentication, and electronic signature capture in their business operations.

- PKI uses a combination of computer software, hardware, and encryption techniques to allow users to securely communicate over computer networks. The Centers for Disease Control has successfully used PKI to authenticate communications between its external parties.

- Knowledge-based authentication tests a users' recall of inherently personal information. eBay uses a form of knowledge-based authentication in its on-line auction operations.

- Electronic signature capture uses computer hardware and software to electronically capture an image of a person's signature, which can be placed within an electronic document. Colonial Life & Accident Insurance Company uses electronic signature capture and has eliminated the need for most paper records.

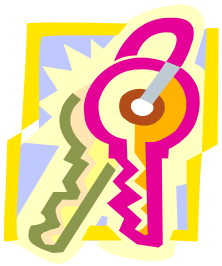
An official at the National Archives and Records Administration (NARA) explained that electronic records storage is a viable archive format. He suggested periodically migrating electronically stored files to newer less expensive storage mediums to help ensure that electronically stored information remains readily accessible and to minimize electronic information storage costs. The NARA official also suggested considering storing data in standard formats that are easily read by most software and require less storage space.

PUBLIC KEY INFRASTRUCTURE

PKI authentication technology has existed for over two decades. PKI is formed by a combination of computer software, hardware, and encryption techniques that allow a user to complete secure communications and transactions over computer networks.

Entities using PKI benefit from the convenience and speed of the internet. They also benefit from knowing that critical information is guarded from unauthorized use. PKI protects information in several ways because it:

- authenticates the identity of users,
- verifies that the message has not been tampered with,
- protects information from interception during transmission, and
- minimizes the risk of an electronic transaction later being denied as a forgery.



PKI is based on an electronic key pair. The key pair consists of a unique private key and a corresponding public key. The keys are encrypted and mathematically related. In a PKI system, the private key must be closely guarded and kept secret by its owner. However, the corresponding public key can be freely sent to others within the PKI network who need to communicate securely with the private key holder. A user's public key may be broadly distributed for others to use because only the holder of the related private key can decrypt a message. In practice, the sender encrypts a message with the intended recipient's public key. Because of the mathematical relationship between the user's private key and public key, only the recipient holding the related private key can decrypt or read the message.

Certificate authorities (CAs) act like a passport office for the digital world. The CA is responsible for validating a potential key holder's identity. Additionally, the CA creates and issues to users digital certificates, which house the public key. A PKI system must rely on a trusted CA to distribute public keys and authenticate the identity of the user associated with the key pair. The CA functions are sometimes contracted to a third party.

Just as CAs act as a passport office for the digital world, the digital certificates created by a CA, act as on-line passports or electronic credentials. The digital certificate, an electronic file, binds a user's identity to their public key. The CAs place the user's public key and other identifying information into each digital certificate and then encrypt it to protect against tampering or alteration. A typical digital certificate, which is unique to each user, contains the user's name, public key, and the CA's name. Digital certificates are installed on a user's computer or network to automate the distribution of the public keys, which are derived from its mathematically related private key. A user's private key also resides on their computer or server.

Despite the apparent complexity of PKI, the actual authentication process requires little user interaction. For example, to initiate a PKI based message, a user simply logs into a network using special software installed on their computer. Once logged in, the PKI electronically authenticates the user behind the scenes and allows for secure communication among parties.

Centers for Disease Control Uses PKI

The Centers for Disease Control (CDC), in Atlanta, Georgia, implemented PKI in 1999. The CDC's Secure Data Network (SDN) uses PKI to authenticate communications between its external partners. The CDC's PKI partners include hospitals, doctors, nurses, and health departments around the world that need to obtain and provide sensitive medical information. Because of the highly sensitive nature of the information being transmitted, CDC recognized the need for PKI to ensure user identity and data integrity. CDC collects enrollment data on prospective PKI users and confirms the potential user's identity. Once the CDC approves a new user, it uses a third party CA to issue and administer the digital certificates. The CA also provides the resources and services to authenticate a message sent using CDC's PKI.

One of the biggest challenges CDC faced was configuring partner's hardware and software for use with its SDN. Without compatibility, secure authenticated communications cannot occur. In the personal opinion of a CDC official, if an organization has a sufficient volume of digital certificates, it should dedicate information technology (IT) staff to implement and support its PKI. The CDC's PKI system has also been developed so it may be integrated, as needed, into future eGovernment projects.

KNOWLEDGE-BASED AUTHENTICATION

Knowledge-based authentication is the most commonly used method for verifying a user's identity in a computer environment. Typically, at a computer logon prompt users are first asked to identify themselves and then are asked a series of challenge questions to authenticate themselves. The challenge questions should be unique to the individual user and not commonly known by others.

Knowledge-based authentication is relatively easy for an entity to implement, since it does not require users to have specialized hardware or software. In most cases, users can be authenticated using a standard personal computer linked to the internet. Other advantages are that the users can protect their knowledge by simply remembering a few key pieces of information, the knowledge or information is portable, and, if necessary, can be easily changed.

Passwords are the most common form of knowledge-based authentication and may provide adequate protection of electronic information. Passwords are widely used by persons with personal computers and internet access to conduct on-line transactions. Banks, credit card companies, utilities, brokerage houses, and on-line retailers use passwords to help authenticate their on-line customers and provide access to their internet-based services.

Although user friendly, password-based authentication can sometimes be insufficient in preventing unauthorized access. If not designed properly, password-based authentication may be vulnerable to "hackers" using software designed to guess common passwords. To increase security, password-based authentication systems should be designed to prevent multiple guessing and to identify and prevent the use of easily guessed passwords. Although, a well designed system is vital in protecting access, users themselves may be the weakest security link in a knowledge-based system. To improve security, users should be educated to protect their password from unauthorized use and to make their password sufficiently complex. Password integrity may be improved by the use of numbers, special characters, misspelled words, and nondictionary words. Additionally, users should be cautioned not to write and store their password next to the computer or to share it with others.

A more advanced application of knowledge-based authentication is available to cope with the increasing challenge of authenticating on-line users. VeriSign, Inc. (VeriSign) located in Mountain View, California, provides a unique third party authentication service to entities conducting on-line transactions that require a high level of security. VeriSign's product, Consumer Authentication Service (CAS), asks users for multiple pieces of personal information and then cross checks the responses against over 50 databases to authenticate them. CAS is fully supported by VeriSign and is designed to be integrated into existing internet browsers and computer networks.

When an on-line transaction is initiated, CAS, in real time, cross checks personal information, such as home addresses, phone numbers, driver's license numbers, birth dates, and even email addresses to authenticate a user. For high-value transactions or those involving sensitive information, CAS provides a higher level of validation by comparing responses to questions requiring more personal financial information, such as account numbers, account balances, and credit limits prior to authorization. CAS's communication with the external databases is encrypted for security. Furthermore, CAS performs all identity checks in compliance with key privacy and security regulations.

eBay Implements Third-Party Knowledge-Based Authentication

eBay, in San Jose, California, implemented CAS to authenticate its on-line auction members. eBay is the world's largest on-line trading entity, where millions of people buy and sell millions of items every day. Potential buyers search for items and place

bids on those items they are interested in purchasing. Sellers have the ability to market their product to millions of daily on-line visitors. Since eBay's business involves a large number of users and a high volume of transactions, they were aware of the potential risk of identity fraud. eBay decided to implement the CAS system because it enables them to better assure the identity of both new sellers and sellers of high-dollar value goods.

In the fall of 2002, eBay implemented their Identification (ID) Verify program, powered by VeriSign's CAS. The ID Verify program allows eBay customers to establish proof of their identity to eBay and other auction members. Once authenticated, ID Verify members receive a special icon in their user profile, which can be viewed by other auction members. ID Verify members receive additional auction privileges. For example, ID Verify members may bid on higher dollar value transactions and sell items using more exclusive listing features. Effectively, the ID Verify icon serves as a calling card to other auction members helping them to identify a trusted trading partner. The ID Verify program is available to on-line auction members in the United States, Puerto Rico, the U. S. Virgin Islands, and Guam.

A member's privacy is important to eBay. The information provided to eBay during the ID Verify enrollment process is neither stored by eBay nor by VeriSign. Instead, VeriSign's CAS only compares customer's responses to external and consumer and business databases. CAS assigns a numerical score to the comparison, which indicates its confidence in the information provided. Although CAS assigns a score, eBay is responsible for interpreting the score and deciding whether an applicant is accepted into its' ID Verify program. Customer responses to the CAS's credit related questions do not affect their credit ratings. The on-line ID Verify process is protected by a secure and encrypted internet connection to help ensure users' privacy is maintained.

ELECTRONIC SIGNATURE CAPTURE

Electronic signature capture technology utilizes both computer hardware and software to capture a person's physical signature electronically. An electronic signature pad and related software are used to capture an individual's signature and then place an image of the signature within an electronic document. Signature pads are commonly found in retail stores as part of a system to process credit card transactions. Electronic signature capture is not limited to the retail industry. Other industries, such as insurance, have also embraced this technology.

Colonial Life & Accident Insurance Company Implemented Electronic Signature Capture

Like SSA, some insurance companies have many signature requirements for their paper records. Colonial Life & Accident Insurance Company (Colonial), an insurance company located in Columbia, South Carolina, processes over 700,000 signed applications a year and operates in 49 states. Prior to implementing electronic forms, paper documents were sent between agents and Colonial's home office to facilitate its insurance underwriting. Important paper records were transcribed into electronic format. This process was inefficient, subject to keying errors and time delays.

Prior to implementing electronic signature capture, Colonial began using electronic versions of its insurance documents. The electronic documents were installed on its agents' laptop computers in a process called electronic application submission. Despite this advancement, the physical signature of both agents and the insurance applicant were still required. As a result, paper documents were still being created and processed. In 1999, Colonial implemented electronic signature capture using electronic signature pads connected to the agents' computers. With the addition of the electronic signature pads, Colonial effectively eliminated the need to handle most paper insurance applications.

One of Colonial's concerns in transitioning to electronic signature capture was whether agents and clients would accept the signature pads, since they were more comfortable using conventional paper forms. To further ease transition from paper forms to electronically captured signatures, Colonial decided to place a small piece of paper over the electronic signature pad so that users may sign the paper with an ink pen, in a familiar manner. As the paper is signed by the conventional pen, a simultaneous electronic version of the signature is also captured on an electronic pad. The presence of the piece of paper and ink pen helped both agents and clients feel better about adapting to the new electronic technology.

Today, Colonial processes approximately 80 percent of its new insurance policies using electronic forms and electronic signature capture. Colonial realized dramatic benefits transitioning to electronic application process. Among the benefits Colonial realized was reduced processing costs, improved timeliness, increased productivity, and enhanced customer service.

Electronic Signature Capture Can Prove an Individual's Identity

In addition to capturing an image of an individual's signature, electronic signature pads can be used to prove someone's identity. In a more advanced application of electronic signature capture, users may prove their identity by the way

they physically sign their name. This electronic signature capture technology uses special software that measures the shape, speed, pressure, and stroke of an individual's signature. A sample of three to six signatures captured on an electronic signature pad is needed to create an electronic profile of the user's writing style.

The angle in which the pen is held, the pressure applied in signing, and the signature style are all captured and stored in an electronic profile. This profile is stored in a computer system for comparison with future electronic pad transactions. In subsequent transactions, when a person signs an electronic signature pad, their signature is electronically compared to their profile to authenticate them. Once authenticated, an image of the signature is also placed into a related electronic document. Together the image and the associated characteristics become the individual's legal signature.

Communication Intelligence Corporation (CIC), in Redwood Shores, California, manufactures handwritten signature software similar to that described for Colonial and has developed technology to authenticate electronically captured signatures. This technology is referred to as eSignature and enables an organization to:

- identify an individual based on their signature,
- capture a legally binding and regulatory compliant electronic handwritten signature,
- electronically seal the signature and document content together to prevent and detect tampering, and
- minimize the risk of having an electronically captured signature later be denied as a forgery.

In addition to authenticating a user in a financial transaction, this technology provides a verifiable electronic signature that can replace passwords. This method of authentication provides an added level of security to simple passwords. Although, passwords can be given to other individuals, stolen, or forgotten, a signature is unique to an individual and cannot be forgotten. Potentially, this technology can replace passwords to access networks, secure laptop or handheld computers, or even secure individual files on a network.

Nationwide Building Society is Identifying Customers by their Electronic Signature

In the public and private sectors, the ability to capture signatures, as well as verify the identity of users in an electronic transaction is becoming more important. One company, Nationwide Building Society (NBS), a banking institution in the United Kingdom, has recognized the merits of electronically capturing and authenticating its customer's signature to complete a transaction. For 2 years, NBS researched various methods to authenticate its customers and selected CIC's eSignature technology.

NBS has 70 processes that require a signature and produce large volumes of paper. NBS expects to see dramatic improvement in transaction efficiency and fraud prevention using eSignature. NBS also anticipates significant cost savings through paper reduction. In fact, NBS expects to achieve a return of its investment within 3 years through paper reduction and fraud prevention.

NBS has started the beginning phases of implementing the eSignature technology. Initially, electronic signature pads will be used to sign forms. In the near future, NBS expects to implement eSignature for customer cash withdrawals and to open bank accounts. In a recent test trial of 120 staff, NBS found it was impossible for participants to forge a signature just by copying it, and the electronic pad system neither rejected a legitimate signature, nor accepted one that was false.

ELECTRONIC RECORDS STORAGE

As Government and business entities increase operations in an electronic records environment, the number of electronic records they need to store will continue to increase. These entities recognize the significant cost of storing and retrieving paper based records. As a result, some entities are exploring electronic records archives as an alternative storage medium. Records experts acknowledge that the electronic storage of documents can be cost-effective, but because clear policies, technical standards, and resources are often lacking, some agencies are hesitant to "go paperless."

The National Archives and Records Administration (NARA) is responsible for assisting Federal agencies in maintaining adequate and proper documentation of Government policies and transactions.[3] NARA, as well as the Library of Congress, is working to address the issue of preserving electronic information over the long term. According to NARA officials, electronic records policy is still evolving, but fundamentally, electronic records retention is inherently a records management issue dealing with efficiency and the protection of rights.

Converting Paper Records into Electronic Form

The process of converting paper documents into electronic form is referred to as imaging. Imaging is the process by which a paper document is converted to a computer-readable digital-image file. To obtain an image, a device, such as a scanner, is used to capture an electronic image of an original document.

[3] NARA is an independent Federal agency, authorized under 44 U.S.C. § 2101 et seq., whose mission ensures, for the citizen and the public servant, for the President and Congress and the Courts, ready access to essential evidence.

Special software then saves the image as a computer file to store the data. Once created, the computer files are stored in an electronic medium. The most common types of storage mediums are magnetic tapes and discs, and optical media, such as CD-ROM. The amount of time and labor needed to scan or image a document is dependent upon how efficiently the paper records can be retrieved and processed into the scanner.

An official at NARA explained that electronic records storage is a viable archive format. According to this official, original paper records may be destroyed after they are converted to electronic format, if adequate safeguards are in place to verify the authenticity and accuracy of an original scanned document and sufficient safeguards are in place to protect against unauthorized alteration or destruction of new archive records. Moreover, he explained that a correctly scanned image may be as reliable as the original document and is also considered an official record. Despite embracing electronic records storage, the NARA official cautioned that the storage medium used today will likely change in the future. To help ensure that electronically stored information remains readily accessible and to minimize electronic information storage costs, the NARA official recommends periodically migrating electronically stored files to newer less expensive storage mediums.

The NARA official also expressed concern with storing information in software specific (proprietary) electronic file formats. He cautions that information stored in present proprietary file formats may not be accessible by future computer software. In the long term, proprietary file formats may become obsolete, manufacturers may not support software used to read the file formats, or newly developed software may not be backward compatible to read earlier file formats. The official suggests storing data in standard formats that are easily read by most software and require less storage space.

CONCLUSIONS AND RECOMMENDATIONS

We acknowledge that SSA management has tested or implemented some aspects of the electronic records authentication practices discussed in this report, especially in the areas of PKI and knowledge based authentication. We are encouraged that SSA continues to refine and improve its current electronic records authentication techniques. We believe the current practices discussed in this report are compatible with SSA's electronic service delivery initiative. Moreover, we believe the authentication successes realized by the organizations we contacted warrant SSA’s consideration of their practices. We recommend that SSA:

1. Consider these organizations’ use of PKI, knowledge-based authentication, and electronic signature capture as they relate to the agency’s electronic service delivery initiative.

2. Ensure that its electronic records storage procedures specify file formats that remain readable by future generations of software.

AGENCY COMMENTS

In commenting on the draft report, SSA agreed with our recommendations. SSA also provided additional comments that we incorporated in the report as appropriate. See Appendix B for the full text of SSA comments.

James G. Huse, Jr.

Appendices

Background, Scope and Methodology

Background

The Social Security Administration (SSA) is currently testing several uses of public key infrastructure (PKI) to support its business processes. For example, PKI is being tested to electronically report annual wages and medical information. Also, SSA is presently using forms of knowledge based authentication techniques to prove the identity of its beneficiaries. For example, once authenticated, beneficiaries can change their mailing address, check their Social Security benefits, and apply for direct deposit over the internet.

In addition to the above examples, SSA stated that it has performed extensive work in the area of electronic records authentication. Regarding this work, SSA explained that it has obtained legal opinions from its General Counsel, established policies, and implemented best practices. Moreover, SSA indicated that it is an active participant in the E-Authentication project and the Electronic Records Management project under the E-Government Initiative of the President's Management Agenda.

Organizations conducting on-line transactions must verify the identities of their users to avoid potential fraud-related losses. Identity fraud is one of the fastest growing crimes today and is often perpetrated via computers and databases. We consulted Frank W. Abagnale, founder of the secure documents company Abagnale & Associates in Washington, DC. Mr. Abagnale is a:

- world-famous former con artist,
- bestselling author of *Catch Me If You Can* and *The Art of the Steal,* and
- long-term consultant (25 years) to the Federal Bureau of Investigation's (FBI) financial crimes unit.

Mr. Abagnale recommended organizations guard against potential loss and fraud created by identity theft. He warned, "What one man creates, another can foil." In creating an authentication system, Mr. Abagnale explained that there is often a trade off between usability and security. Therefore, he recommends a comprehensive risk assessment and business analysis should be performed to match the sensitivity of the data with the appropriate level of authentication.

Scope and Methodology

This review was designed to identify current practices in electronic records authentication that may enhance SSA's electronic service delivery initiative. We interviewed the following entities to gain an understanding of their electronic records authentication technology or techniques. See Table 1 on the following page for a brief

description of the entities included in our review. We selected these organizations because they have either developed or successfully used authentication technologies.

- Centers for Disease Control, Atlanta, Georgia
- Colonial Life & Accident Insurance Company, Columbia, South Carolina
- Communication Intelligence Corporation, Redwood Shores, California
- eBay, San Jose, California
- Nationwide Building Society, United Kingdom
- VeriSign, Inc., Dulles, Virginia

We performed our work with the entities above and at the Office of Audit, Atlanta, Georgia. We conducted our review from April through July 2003 in accordance with generally accepted government auditing standards.

The organizations we contacted have reviewed the information we presented in this report and have authorized its use.

Table 1: Description of Entities Contacted

Entity	*Business Purpose*
Centers for Disease Control (CDC)	The CDC is recognized as the lead Federal agency for protecting the health and safety of people—at home and abroad, providing credible information to enhance health decisions, and promoting health through strong partnerships.
Communication Intelligence Corporation (CIC)	CIC develops and provides electronic and digital signature solutions, which authenticate electronic handwritten signatures and original content of on-line digital documents.
Colonial Life & Accident Insurance Company (Colonial)	Colonial offers a broad line of insurance products, including disability, accident, life, cancer, critical illness and hospital confinement.
eBay	eBay is the world's largest on-line trading community, where millions of people buy and sell millions of items every day.
Nationwide Building Society (NBS)	NBS offers a range of retail financial services, including mortgages, savings, current accounts, life assurance and investment products, personal loans, and household insurance.
VeriSign, Inc. (VeriSign)	VeriSign delivers critical infrastructure services that make the Internet and telecommunications networks more intelligent, reliable, and secure.

Agency Comments

SOCIAL SECURITY

MEMORANDUM 113-24-1069

Date: January 22, 2004 Refer To: S1J-3

To: James G. Huse, Jr.
Inspector General

From: Larry W. Dye /s/
Chief of Staff

Subject Office of the Inspector General (OIG) Draft Management Advisory Report "Current Practices in Electronic Records Authentication" (A-04-04-24004)—INFORMATION

We appreciate OIG's efforts in conducting this review. Our comments on the draft report content and recommendations are attached.

Please let me know if you have any questions. Staff inquiries may be directed to Candace Skurnik, Director, Audit Management and Liaison Staff on extension 54636.

Attachment:
SSA Response

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT MANAGEMENT ADVISORY REPORT "CURRENT PRACTICES IN ELECTRONIC RECORDS AUTHENTICATION" (AUDIT NO. A-04-04-24004)

We appreciate the opportunity to review and comment on the draft report. Although SSA had the first production of Public Key Infrastructure (PKI) application on the Federal e-Authentication infrastructure, we acknowledge that we must be vigilant in ensuring that the best approaches are employed. We agree with the recommendations and will continue to consider the use of PKI, knowledge-based authentication and electronic signature capture in future electronic service delivery initiatives. Additionally, we will endeavor to ensure that electronic records storage procedures specify file formats that remain readable by future generations of software.

We appreciate your efforts in providing this broad overview of authentication practices and electronic records storage in a few public and private organizations. As mentioned at the exit conference, however, we had anticipated the report would provide more details on the pros and cons of each authentication method. In addition, while the report provides a cursory review of technologies used for encryption, identity authentication and access control, we believe that some of the definitions and examples confuse the application of these technologies for use in authentication, authorization and records management.

Specific areas requiring clarification include:

- the area that discusses the use of Public Key technology for encryption (cryptographic transmission security) and authentication which requires a PKI certificate be issued for the express purpose of digital signature activity,
- the discussion that electronic signature capture conveys authentication of identity; it is not clear in distinguishing verification of records versus authentication of individuals' identities. On page 3 – 4th bullet – "eliminates unauthorized access…." PKI (or any other authentication methodology) coupled with an appropriate and robust authorization mechanism helps to eliminate unauthorized access to "resources." There is a common misunderstanding where "authentication" and "authorization" are used interchangeably. Authentication provides a measurable level of assurance of properly identifying an individual; while authorization controls what resources that authenticated individual can access and what roles they may take with those allowed resources.

Also, as you may already know, the General Services Administration (GSA), in coordination with the Office of Management and Budget (OMB), has the lead for developing a government-wide E-Authentication Policy that will establish a standard framework for assessing e-government electronic transaction authentication requirements. The proposed E-Authentication Policy establishes a four-level approach for authentication to ensure trustworthy electronic transactions and to fulfill Federal privacy and information security requirements. It also specifies a three-step implementation process that includes: 1) conducting a risk assessment in accordance with the guidance explained in Part II of the Government Paperwork Elimination Act and Section 2 of the proposed Policy; 2) determining the appropriate assurance level based upon

the identified risks; and 3) deploying the corresponding technology solution based on the e-authentication technical guidance to be issued by the Department of Commerce's National Institute of Standards and Technology (NIST).

On December 16, 2003, OMB released the E-Authentication guidance for all Federal agencies. That guidance updates the earlier guidance issued by OMB under the Government Paperwork Elimination Act of 1998, 44 U.S.C. § 3504 and implements section 203 of the E-Government Act, 44 U.S.C. ch 36. It also mandates that all Federal agencies categorize all existing transactions/systems requiring user authentications into one of the OMB described assurance levels:

- Systems classified as "major" must be completed by December 15, 2004.
- New authentication systems should begin to be categorized, as part of the system design, within 90 days of the completion of the final E-Authentication Technical Guidance issued by the NIST.

Given GSA's and OMB's efforts in this area to date, we expect that Federal agencies will be required to take actions well beyond those recommended in this report.

Finally, while we recognize that the purpose of the review was to identify and evaluate electronic records practices of other entities, the conclusions statement that begins "SSA management has tested or implemented some aspects of the electronic records authentication practices," implies that the Agency has done limited work in this area. The report should highlight the fact that we have done extensive research including obtaining General Counsel opinions, establishing internal policies and implementing best-practices based on our work in the field of electronic authentication. We are an active participant in both the E-Authentication project and the Electronic Records Management project, under the E-Government Initiative of the President's Management Agenda.

Our specific comments to the recommendations are provided below.

Recommendation 1

SSA should consider these organizations' use of PKI, knowledge-based authentication, and electronic signature capture as they relate to the Agency's electronic service delivery initiative.

Response

We agree. We have already exceeded the recommendations of this report through participation in both Government and private industry organizations and standards bodies dealing with electronic authentication technologies and electronic records management. Our Office of Electronic Services (OES) investigates, analyzes and pilots the application of technologies in our business processes. They also monitor private industry and government-wide activities and policies to ensure that we investigate potential technologies that will provide better service to the public. Additionally, they provide support through installation, training and support of technologies throughout the field structure as they are made available.

Recommendation 2

SSA should ensure that its electronic records storage procedures specify file formats that remain readable by future generations of software.

Response

We agree. Electronic records are an emerging field for the National Archives and Records Administration (NARA). They have established record management criteria and endorsed the Department of Defense's (DOD) 5015 as a record management system that meets their requirements. Our records management staff are working with the Office of Systems to ensure that Agency specifications for system design and management meet all NARA requirements including that electronic storage be in a viable archive format easily read and requiring minimum storage space. The Office of Systems has determined that their standard architecture meets these basic requirements. They have also developed a matrix that cross walks their plan for our electronic record management system with the NARA requirements and the criteria established by DOD to demonstrate that the evolving SSA record management system will meet NARA's requirements for electronic recordkeeping.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Mark Bailey, Director (816) 936-5591

Frank Nagy, Audit Manager (404) 562-5552

Staff Acknowledgments

In addition to those named above:

David McGhee, Auditor

For additional copies of this report, please visit our web site at www.ssa.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 965-1375. Refer to Common Identification Number A-04-04-24004.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Subcommittee on Human Resources

Chairman and Ranking Minority Member, Committee on Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Government Reform and Oversight

Chairman and Ranking Minority Member, Committee on Governmental Affairs

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

Office of Audit

The Office of Audit (OA) conducts comprehensive financial and performance audits of the Social Security Administration's (SSA) programs and makes recommendations to ensure that program objectives are achieved effectively and efficiently. Financial audits, required by the Chief Financial Officers' Act of 1990, assess whether SSA's financial statements fairly present the Agency's financial position, results of operations and cash flow. Performance audits review the economy, efficiency and effectiveness of SSA's programs. OA also conducts short-term management and program evaluations focused on issues of concern to SSA, Congress and the general public. Evaluations often focus on identifying and recommending ways to prevent and minimize program fraud and inefficiency, rather than detecting problems after they occur.

Office of Executive Operations

The Office of Executive Operations (OEO) supports the Office of the Inspector General (OIG) by providing information resource management; systems security; and the coordination of budget, procurement, telecommunications, facilities and equipment, and human resources. In addition, this office is the focal point for the OIG's strategic planning function and the development and implementation of performance measures required by the *Government Performance and Results Act*. OEO is also responsible for performing internal reviews to ensure that OIG offices nationwide hold themselves to the same rigorous standards that we expect from SSA, as well as conducting investigations of OIG employees, when necessary. Finally, OEO administers OIG's public affairs, media, and interagency activities, coordinates responses to Congressional requests for information, and also communicates OIG's planned and current activities and their results to the Commissioner and Congress.

Office of Investigations

The Office of Investigations (OI) conducts and coordinates investigative activity related to fraud, waste, abuse, and mismanagement of SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, physicians, interpreters, representative payees, third parties, and by SSA employees in the performance of their duties. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Counsel to the Inspector General

The Counsel to the Inspector General provides legal advice and counsel to the Inspector General on various matters, including: 1) statutes, regulations, legislation, and policy directives governing the administration of SSA's programs; 2) investigative procedures and techniques; and 3) legal implications and conclusions to be drawn from audit and investigative material produced by the OIG. The Counsel's office also administers the civil monetary penalty program.