

## **ARIA INTERNAL ELECTRONIC SIGNATURES POLICY**

### **1. PURPOSE.**

This policy establishes the criteria for the use and validity of electronic signatures associated with electronic transactions within the Automated Research Information Administrator heretofore described as ARIA.

### **2. SCOPE AND APPLICABILITY.**

This policy applies to any electronic transaction originated by any user of ARIA where that transaction involves providing approval, authorization, or certification, via the use of electronic signature, for actions or data.

### **3. BACKGROUND.**

#### **a. General**

- (i) Innovations in computer technology now allow the creation, processing and maintenance of documents in electronic form -- without requiring creation of corresponding paper media.
- (ii) Automated information processing is rapidly becoming the preferred mode for management and transfer of information in business and government. Automation of administrative procedures has demonstrated that:
  - (a) Information can be processed more quickly
  - (b) Costs of re-keying data are mitigated
  - (c) Data accuracy is increased
- (iii) Procedures for the use of electronic signatures in creating and processing documents must provide adequate safeguards for the application, transmission, verification, and security of a signature and any accompanying data or information. If security profiles are modified, the system should be equipped with an audit trail capability to provide the User ID, time and date of the last person who made the modifications.
- (iv) Pursuant to Par. 4, **AUTHORITIES**, of this policy, as such information migrates into an electronic environment, it is essential to ensure that all official documents are developed, processed, and maintained consistent with applicable Federal and Agency policies regarding electronic recordkeeping.

b. Existing Technology Areas As Management Controls for Electronic Signatures

The following technology areas used individually or in concert as controls can provide effective electronic signature systems:

(i) Signature authentication allows users to verify the approval authority of transmission. It is usually used in combination with other technologies to provide a complete electronic signature system. Signature authentication methods include:

- (a) Personal identification numbers (PINs)
- (b) passwords
- (c) facsimile signatures
- (d) token card readers
- (e) message authentication coding (MAC)
- (f) MAC incorporating encryption techniques, e.g. through the use of public or private keys.

(ii) Message authentication provides the ability to confirm that the message received is exactly the same as the message that was sent. A major concern associated with electronic forms and signatures is an unauthorized user's ability to change an electronic form after it has been signed.

- (a) Message authentication systems use varying procedures to calculate a message authentication code (MAC) based on the contents of the message. Some of these processes may involve cryptographic techniques. For example, message authentication systems may use private key encryption to calculate the MAC, requiring that both the sender and receiver know the key.
- (b) If the message changes, the MAC code calculated on the receiver's side will be different from the attached MAC code calculated on the sender's side.
- (c) Message authentication may provide two forms of security. It:
  - (1) Verifies the information has not been altered from the moment the MAC was generated to the time it was checked.
  - (2) May also assure the receiver of the sender's identity, e.g. through shared knowledge of the secret key used to calculate the MAC.

(3) Data encryption systems conceal message meaning by changing intelligible messages into unintelligible ones to everyone except the transmitter and receiver. Data encryption:

(a) Can be used to safeguard signatures and signature authentication codes from disclosure during transmission and when data files containing signatures are stored.

(b) Requires the use of keys to encrypt and decrypt data.

(c) Can use public key, private key, or secret key encryption algorithms.

(4) Access control systems are designed to limit access to computer systems, including operating system files, and applications, including application programs and data files. Limiting access to systems and applications limits the population of users that can actually append a signature code to a message. Access control systems, at a minimum, should provide user identification, login control, access authorization, and auditing capabilities.

#### 4. AUTHORITIES.

- a. Internal Control Systems, OMB Circular A-123, August 16, 1983
- b. The Paperwork Reduction Act of 1980 (P.L. 96-511)
- c. United States Code 31-USC-1501
- d. The Federal Managers Financial Integrity Act of 1982 (PL 97-225, approved 9/8/1992)
- e. Federal Records Management, National Archives and Records Administration (NARA) 36 CFR 1220
- f. Review and Evaluation, NARA 41 CFR 201-22
- g. The Computer Matching and Privacy Act of 1987, 5-USC-522a (as amended)
- h. Management of Federal Information Resources, OMB Circular A-130
- i. Computer Security Act of 1987
- j. FIPSPUB46-1 -- Data Encryption Standard; Jan. 22, 1988

- k. FIPSPUB140A -- General Security Requirements for Equipment Using the Data Encryption Standard; April 14, 1982
  - l. EPA 2100 Information Resources Management Policy Manual 1987
  - m. EPA Directive 2182: EPA System Design and Development Guidance, Volumes A&B, plus the supplement: Development of Image Processing Systems in the EPA; 1989/1990
  - n. EPA Directive 2195: EPA Information Security Manual;
5. POLICY.

ARIA is designed to support the implementation of integrated electronic processing applications that expedite the workload and reduce duplicative activities, consistent with applicable Federal and agency policies regarding electronic recordkeeping and security.

- a. For all ARIA transactions involving the use of electronic approval, signature and distribution procedures, an electronic signature will be deemed as legally binding as a paper signature.
- b. When an electronic message containing a signature is signed, transmitted, and received, the following requirements must be met:

(1) Signature Authentication:

- (a) The electronic signature must establish sender/user authenticity
- (b) It must be possible to assure with a reasonable degree of certainty that the sender's signature has not been forged
- (c) Sufficient audit trails must be provided to resolve disputes, with a reasonable degree of certainty, involving cases where an individual disavows sending a message

(2) Message Authentication:

- (a) It must be possible to assure, with a reasonable degree of certainty, that either a document and its signature have not been changed after it is signed or that any changes made to the document are recorded in a human readable audit trail.

- (3) Transactions involving the use of electronic signatures must incorporate signature and message authentication, as above, and may incorporate the following additional considerations:
  - (a) The need for the signature on a document to be obscured from disclosure during transmission (i.e., data encryption)
  - (b) The need for only a few individuals to have access to signing, processing, or viewing capabilities (i.e., access control)
- (4) Only digital signatures are addressed by this policy. Analog, or facsimile signatures are not necessarily electronic, may be forged, and will not be considered valid for determining signature authenticity.

6. RESPONSIBILITIES.

- a. The ARIA Project Manager, and Senior Programmers are responsible for:
  - (1) Periodic review of ARIA's adherence to this policy
  - (2) Conducting a risk analysis and vulnerability assessment every three years to ensure the security of electronic records
  - (3) Identifying a specific technical approach for all required technology areas that cost-effectively addresses the risks of the application
  - (4) Determining the level of security required for electronic signatures and developing, or modifying, the System Security Plan to incorporate electronic signature issues
  - (5) Ensuring that controls are in place, evaluated regularly, and practiced to ensure that this policy is carried out for using electronic signatures
- b. The Institutional Review Board (IRB) is responsible for:
  - (1) Providing training and awareness about the policy
  - (2) Providing guidance and assistance in implementing this policy
  - (3) Ensuring that information security and Privacy Act issues have been met
  - (4) Receiving and responding to waiver requests

(5) Periodically reviewing electronic records to ensure that they are being maintained in accordance with applicable Federal and Agency policies and procedures

(6) Re-evaluating/re-validating the policy within 5 years of approval

## 7. DEFINITIONS.

Access Control - A method of providing security designed to limit access to computer systems and applications. Types of access control include:

- \* User Identification Codes
- \* Login Control
- \* Auditing

Auditing - The practice of recording specific security relevant events. By recording these events, it is possible to detect intrusion attempts by unauthorized users, monitor undesirable activity at a site, or general auditing of various aspects of systems usage. For example, events that should be audited include:

- \* Selected uses of files and hardware devices
- \* Logins, logouts, and break-in attempts
- \* Activities of specific users
- \* Changes to passwords
- \* Changes to security profiles

Automated Information Processing - The electronic creation, processing, and exchange of information without the creation of corresponding paper media.

Data Decryption - The process of converting ciphertext (an encrypted message) into readable form.

Data Encryption - A security method that conceals message meaning by changing intelligible messages to unintelligible ones. Encryption is the process in which plaintext messages are converted into apparently random nonsense, called ciphertext, using an encryption algorithm and a data encryption "key".

Data Encryption Key - A bit string that controls a data encryption algorithm. The data encryption algorithm will produce a different output depending on the specific key used.

Electronic Record - Any information that is recorded in a form that only a computer can process and that satisfies the definition of a Federal record in 44 USC 3301 (see Records below).

Electronic Reporting - The computer-to-computer exchange of information in a standard format via either an electronic (e.g., dial-up telecommunications links, dedicated computer-to-computer links) or magnetic (e.g., diskettes, tapes) medium.

Electronic Signature - A data element, entered into a computer by an authorized person, who is used for noting the ownership, approval, acceptance, or certification of another object (e.g., a document or message). Electronic signatures provide the same validation and authentication capabilities as hand written signatures.

Encryption Key Management - The generation, distribution, entry, and destruction of encryption keys. While data encryption algorithms are publicly known, depending on the specific key used, a unique output will be produced. Therefore, it is the encryption key that provides the desired security. Two key management systems exist:

- \* Private key management
- \* Public key management.

Form - For the purpose of this policy, any paper or electronic document with blanks for the insertion of data or information that requires approval involving signature certification.

Login Control - Specifies the conditions users and programs must meet for gaining access to a system. For example, a user usually requires a valid user ID and password before access to a system is provided. Additional methods used to control login include:

- \* Type of computer login (e.g., local, dial-up, remote, network, batch)
- \* Type of terminal or remote computer
- \* Time of day/day of week.

Message Authentication - A method of detecting changes to a message after it has been signed electronically. After signing a message, the sender calculates a Message Authentication Code (MAC) based on the contents of the message. This code is appended to the message and transmitted. The message recipient performs the same calculations on the received message. If the calculated MAC and the received MAC are the same, the message was not altered after the message was signed.

Message Authentication Code (MAC) - The code used by message authentication systems to validate transmitted messages. This code is calculated by performing a series of mathematical calculations on a signed message.

Private Key - A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and not made public.

Public Key - A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and possibly made public.

Public Key (Asymmetric) Cryptographic Algorithm - A cryptographic algorithm that uses two related keys, a public key and a private key; at least one of the two keys is the cryptographic inverse of the other such that data encrypted by the one key can be decrypted by the other; further, the two keys have the property that given the public key it is computationally infeasible to derive the private key.

Records - (From 44 USC 3301) In records management parlance, this term refers to recorded information of continuing administrative, fiscal, legal, historical or informational value, including published materials, papers, maps, photographs, microfilm, audiovisual, machine-readable materials (ADP tapes/disks) or other documentary material, regardless of physical form or characteristics, made or received by the agency that evidences organizations, made or received by the agency that evidences organization, functions, policies, decisions, procedures, operations or other activities of the Government.

Risk Analysis - The process of methodically and comprehensively examining a system to identify the areas that pose a threat of failure to the system.

Secret Key - A cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities, and not made public.

Secret Key (Symmetric) Cryptographic Algorithm - A cryptographic algorithm that uses a single, secret key for both encryption and decryption.

Signature Authentication - A code, used to identify the sender, appended to a message before transmission. This code is validated by the message recipient. A variety of user authentication techniques exist, including:

- \* Personal identification numbers (PINs)
- \* Passwords
- \* Facsimile signatures.

User Identification Codes (User ID) - A code used to identify system users to applications, data, devices, or services. If an invalid user ID is used, then access to the system or application is denied.

## 8. WAIVERS.

Requests for waivers from specified provisions of the policy may be submitted to the Director of the Institutional Review Board (IRB) Office. Waiver requests must be signed by the relevant Senior Official prior to submission to the Director.

a. Waiver Procedures:

(1) Agency offices must submit any waiver requests to the Director, IRB.

(2) The Director, IRB, has sole authority to grant a waiver.

9. GUIDELINES.

a. Federal Records Management, National Archives and Records Administration (NARA) 36 CFR 1220

b. Data Encryption Standard -- FIPS Publication 46-1, National Institute of Standards and Technology, January 1988

c. Public Key Cryptography, Special Publication 800- 2, National Institute of Standards and Technology, April 1991

10. EFFECTIVE DATE.

a. ARIA has been in compliance with this policy since December 10, 2002.