Building the Archives of the Future

Electronic Records Archive
Security Controls in Support of Digital Authenticity

Jarrellann Filsinger

2 August 2006

Overview

- Electronic Records Archive (ERA)
- Authenticity in the Paper and Digital Worlds
- ERA Security Controls
- Summary
- Questions

Electronic Records Archive

What is ERA?

ERA will be a comprehensive system for

preserving and providing continuing access to any type of electronic record

created anywhere in the U.S. Federal Government

enabling NARA to carry out its mission into the future

Why is ERA Needed?

- ✓Makes Government records available for the future
- ✓Helps NARA capture, preserve, and provide access to Federal records
- ✓Protects records that ensure our rights
- ✓Ensures access to these important records
- ✓Improves how NARA manages the lifecycle of Federal Government records

ERA Security Principles

Authorized Access

Accountability

Integrity

Confidentiality

Sustainability

Authenticity

What are the elements of authenticity?

- **Identity: *we know what the record is.***
  - **E.g., National Commission on Terrorist Attacks Upon the United States. Monograph on Terrorist Financing.**
  - **E.g., the final contract signed by parties, X and Y, on a given date**
- **Integrity: *freedom from corruption***
  - Indicators of Integrity:
    - **Record authentication** *declaration about a record at a given time by a reliable person*
    - **Unbroken chain of custody**
    - ***Trustworthiness*** *of the record keepers*
    - **Adequacy of barriers to alteration**
    - **Others** *…*

Paper Authenticity

What are the elements of Authenticity in paper records?

- Physical control
  - **Closed, locked storage locations**
  - **Monitoring of storage**
- Chain of custody
- Physical evidence
  - **Handwriting, characteristics of specific typewriters**
  - **Ink & paper**
  - **Watermark on the paper**
  - **Seals**
  - **Durability of the medium**
  - **Difficulty of alteration**

Digital Authenticity

What are the elements of digital authenticity?

- ***Information about provenance and original order***
- ***Unbroken chain of custody***
- **Record authentication** *declaration about a record at a given time*
- ***Trustworthiness*** *ability of an information system's accountability and its reliability to produce authentic information*
- **Assurance of intellectual integrity** *authenticating access procedures and documenting successive modifications to the record*
- **Others** *…*

Digital Authenticity in ERA

- Identification and Authentication of persons using a computer system where records reside
- Access Control mechanisms restrict privileged access to authorized persons
- Audit records who, what, when, where a record was accessed
- Integrity an electronic seal preserves integrity by facilitating the detection of modification of a record
- System Assurance enabled by the analysis of physical, administrative, and technical controls to ensure high confidence in the computer system

Identification & Authentication (I&A)

- Identities are verified using one of three generic methods*:*
  - *something they know (type 1)* *a password*
  - *something they have (type 2)* *a token*
  - *something they are (type 3)* *a fingerprint*

- Privileged ERA users use both Type 1 and Type 2
- Other ERA users use Type 1, according to NIST 800-63
- General public ERA users are not authenticated, but have access to publicly available records.

- *Greater assurance is achieved from a combination of type 1 and type 2 mechanisms than either used alone.*

Access Control

- Role-based access control
  - Within NARA, roles are created for various job functions such as record processor or archivist. The permission to perform certain operations are assigned to specific roles. NARA staff (or other system users) are assigned particular roles, and through those role assignments acquire the permissions to perform particular ERA system functions.
- Principle of Least Privilege
  - The principle of least privilege is important for meeting integrity objectives. The principle of least privilege requires that a user be given no more privilege than necessary to perform a job.

Audit

- **Accountability** – Audit Log data can identify which user accounts are associated with certain events.
- **Reconstruction** – Audit Log data can be reviewed chronologically to determine what was happening both before and during an event.
- **Intrusion Detection** – Unusual or unauthorized events can be detected through the review of Audit Log data, assuming that the correct data is being logged and reviewed.
- **Problem Detection** – In the same way that Audit Log data can be used to identify security events, it can be used to identify problems that need to be addressed. For example, investigating system errors, resource utilization, trending and so on.

Integrity

- Electronic seal or message digest is a technique to demonstrate that the content of an electronic document has not been altered.
- Virus detection helps to protect ERA from malicious software.
- Strong authentication and encryption preserves the chain of custody during electronic records transfer.

System Assurance

Analytical techniques evaluate the implications of policies, standards, and procedures; the ramifications of changes; and the potential dangers of refinements.

Provides high confidence that ERA performs as required to meet NARA's mission.

Summary

ERA security principles and controls must be viewed in a systems context – they support one another to achieve high confidence in the ERA system.

Digital Authenticity is very much a research topic that will continue to provide ERA with improvements in the future.

Questions/Comments