Requirements for a Trusted Recordkeeping System

Luciana Duranti

InterPARES Project &
School of Library, Archival and Information Studies,
University of British Columbia

Modern Office

- Hybrid documentary systems
- Digital environments that support the manipulation and repurposing of data
- Obsolescence of systems and media
- Proprietary and idiosyncratic nature of applications

One System

- Printing out is an impediment to the workflow in the office
- Many digital documents are not printable
- Digitization is expensive in the long term
- Courts' decisions have been against routine reproduction

Consequences

- Records are less
  - reliable (manipulability)
  - retrievable (incongruence of classifications/taxonomies)
  - accessible, readable or intelligible (incompatibility and obsolescence)
- It is difficult to prove their authenticity while current
- It is difficult to maintain accountability
- It is difficult to provide for long-term preservation of authentic records

How to deal with this situation

- Developing a records policy, a strategy and a procedure that address separately records and the other digital objects
- Focusing any such policy and strategy on the continuing reliability, accuracy and authenticity of records
- Recognizing that preservation of authentic electronic records is a continuous process that begins at the moment of creation and whose purpose is to transmit authentic information across time and space

Record

Any document created (i.e., made or received and set aside for further action or reference) by a physical or juridical person in the course of a practical activity as an instrument and by-product of it.

Records versus data

- All records are documents
- Document = recorded information
- Information = aggregation of data intended for communication over time or space
- Data = the smallest indivisible meaningful fact

Electronic Record

A record created (i.e., made or received and set aside for action or reference) in electronic form

Identifiable Characteristics of an Electronic Record

- Fixed form (i.e. its binary content is stored so that it remains complete and unaltered, and its message can be rendered with the same documentary form it had when first set aside)
- Unchangeable content
- Explicit linkages to other records within or outside the digital system through a classification code or other unique identifier
- Identifiable administrative context
- Involvement of three persons: an author, an addressee, and a writer
- Participation in or support of an action either procedurally or as part of the decision making process

Other Characteristics

- The relation between a record and a file can be one-to-one, one-to-many, many-to-one, or many to many
- The same presentation of a record can be created by a variety of digital presentations and vice-versa, from one digital presentation a variety of record presentations can derive
- It is possible to change the way in which a record is contained in a file without changing the record

Reliability

The trustworthiness of the record as a statement of facts.

Trust in the accuracy of the content.

Authenticity

Refers to the fact that a record is what it purports to be and has not been tampered with or otherwise corrupted.

Authenticity is the trustworthiness of the record as a record. To verify it, one must verify the identity and integrity of a record.

Authentication

A declaration of authenticity, resulting either by the insertion or the addition of an element or a statement to a record, and the rules governing it are established by legislation.

A means of proving that a record is what it purports to be at a given moment in time.

Threats to authenticity

Authenticity is most at risk when records are transmitted **across space** (that is, when sent between persons, systems, or applications) **or time** (that is, either when they are stored offline, or when the hardware or software used to process, communicate, or maintain them is upgraded or replaced)

Conceptual Framework for Authenticity

- In archival theory and jurisprudence, records that are relied upon by their creator in the usual and ordinary course of business are presumed authentic

- In electronic systems, the presumption of authenticity must be supported by **evidence** that a record is what it purports to be and has not been modified or corrupted in essential respects.

- To assess the authenticity of a record, the preserver must be able to **establish its identity** and **demonstrate its integrity**

Identity of a Record/Data

- It refers to the attributes of a record that uniquely characterize it and distinguish it from other records. These attributes include: the names of the persons concurring in its formation (i.e., author, addressee, writer and originator); its date(s) of creation and transmission; an indication of the matter or action in which it participates; classification code or other unique identifier; as well as an indication of any attachment(s).

- These attributes may be explicitly expressed in an element of the record, in metadata related to the record, or implicit in its various contexts (documentary, procedural, technological, provenancial, or juridical-administrative).

Integrity of a Record

- Its wholeness and soundness. A record has integrity if it is intact and uncorrupted
- A record is intact and uncorrupted if the message that it is meant to communicate in order to achieve its purpose is unaltered
- A record's physical integrity, such as the proper number of bit strings, may be compromised, provided that the content and its required elements of form remain the same
- Integrity may be demonstrated by evidence found on the face of a record, in metadata related to a record/data, or in one or more of its contexts

Hence

It is essential to ensure that the electronic records are clearly identifiable and of demonstrable integrity and that accidental corruption or purposeful tampering have not occurred since their creation.

How do we do so?

How do we do so?

- Maintaining the records in a **trusted record keeping system**
- Understanding that it is **not** possible to keep an electronic record as a stored physical object: it is only possible to maintain the ability to reproduce the record
- Ensuring that the reproduction process is the responsibility of a **trusted custodian** having the authority and the capacity of documenting it thoroughly

Trusted Recordkeeping System

A trusted record-keeping system comprises the whole of the rules that control the creation, maintenance, and use of the records of the creator and that provide a circumstantial probability of the authenticity of the records within the system.

Trusted Custodian

To be considered a trusted custodian, the person responsible for keeping the records must demonstrate that he/she has no reason to alter them or allow others to alter them, and is capable of implementing all of the requirements for a trusted recordkeeping system

Trusted Recordkeeping System

The first requirement of a trusted recordkeeping system is that it is capable of controlling all the records of the creator, regardless of their physical form.

Trusted Recordkeeping System
Controlled management of all records

- Integrated Classification/Taxonomy and Retention System
- Metadata System
- Controlled Disposition System

Trusted Recordkeeping System
Metadata System

A metadata system provides for the expression of the **attributes** of each record in a register, a record profile, or a topic map.

These attributes can be distinguished into categories, the first concerning the identity of records, and the second concerning the integrity of records.

Attributes for the identity of the record

- Names of the persons concurring in the formation of the record, that is: name of author, writer, originator, creator and addressee
- Name of action or matter
- Date(s) of creation and transmission, that is: chronological date, received date, filing date, transmission date(s)
- Expression of documentary context (classification code/unique identifier)
- Indication of attachments

Attributes for the integrity of the record

- Name of handling office/person
- Name of office of primary responsibility
- Indication of types of annotations added to the record
- Indication of technical modifications
- Disposition

Trusted Recordkeeping System

Access Privileges

The recordkeeping system must:

- define and effectively implement access privileges concerning the creation, modification, annotation, relocation, and destruction of records, and
- maintain an audit trail of access to the records systems to control the administration and use of access privileges

Trusted Recordkeeping System

Protective Procedures: Loss and Corruption of Records

The creator should

- establish and implement procedures to prevent, discover, and correct loss or corruption of records,
- maintain an audit trail of every transmission within the recordkeeping system, and
- ensure regular system backup

Trusted Recordkeeping System

Protective Procedures: Media and Technology

The creator should establish and implement procedures to guarantee the continuing identity and integrity of records against media deterioration and across technological change, such as regular migration, microfilming, etc.

Trusted Recordkeeping System

Establishment of Documentary Forms

The creator should establish the documentary forms of records associated with each procedure according to either legal and/or organizational requirements or its own requirements

Trusted Recordkeeping System

Authentication of Records

If authentication is required by the legal system or the needs of the organization, the creator should establish specific rules regarding which records must be authenticated, by whom, and the means of authentication

Trusted Recordkeeping System

Identification of Authoritative Record

If multiple copies of the same record exist, the creator should establish procedures that identify which record is authoritative

Trusted Recordkeeping System

Removal and Transfer of Relevant Documentation

If there is a transition of records from active status to semi-active and inactive status, which involves the removal of records from the electronic system, the creator should establish and implement procedures determining what documentation has to be removed and transferred along with the records

In practice …

- These principles have been captured in various standards, e.g.,
  - Department of Defense (DoD) 5015.2: US federal government vendors
  - Security Exchange Commission (SEC) Rule 17a-4: any financial body
  - Food and Drugs Administration (FDA) 21 CFR part 11: pharmaceutical industry

- Software vendors have developed products which complies to various degrees with such standards and regulation:
  - DoD: 5015.2: TRIM (Tower Software)
  - SEC Rule 17a-4: Centera (EMC)
  - Model REQuirements (MoREQ) for an ERMS: R/KYV (Valid Information Systems)

TRIM

- Care of documents throughout their lifecycle and strong classification/taxonomy features, which enable:
  (a) providing linkages between individual records;
  (b) naming records in a consistent manner over time;
  (c) assisting in the retrieval of all records relating to a particular activity;
  (d) appropriate retention periods for record;
  (e) security protection appropriate for sets of records;
  (f) allocating user permissions for access to or action on particular groups of records

- Capture of the initial context and support of additional context relationships as they evolve greatly facilitates information management and retrieval and inferences of authenticity

EMC Centera

- Designed to meet SEC regulations
- Based on “fixed-content addressing“ — using cryptographic hash functions, a unique fingerprint is calculated from each document
- Provides mathematical assurance that documents are never modified, even if using rewritable media (hard disks)
- Can be used as a back-end to a RMS like TRIM.