Jenkinson Disrupted?
The InterPARES Journey

Luciana Duranti
Director, InterPARES Project
The University of British Columbia
Jenkinson Lecture
London, UK 16 May 2019

Why InterPARES (International research on Permanent Authentic Records in Electronic Systems)?

Characteristics of born digital records:

- Their **content, structure, and form are not inextricably linked**
- The record as a stored entity is distinct from its manifestation on a computer screen, and its **digital components** have to be considered as well as its **documentary form**
- They are **vulnerable** (easy to destroy, lose, corrupt, tamper with, or become inaccessible if not protected) yet **persistent** (forever there, if not purposefully destroyed)
- When we save a record, we take it apart in its digital components. When we retrieve it, we create a copy: there are **no originals** in the digital environment
- **Hence, it is not possible to preserve born digital records: we can only preserve the ability to re-produce or re-create it**

InterPARES Trust

The Goal of InterPARES 1 and 2 (1998-2006)

To develop the body of **theory** and **methods** necessary to ensure that records produced in **databases** and **office systems** as well as in **dynamic, experiential and interactive systems** in the course of artistic, scientific and e-government activities can be created **reliable** and maintained and preserved **authentic**, both in the long and the short term, for the use of those who created them and of society at large, regardless of technology obsolescence and media fragility.

Need for Shared Concepts and Terminology

Team members:

- **From countries in 5 continents** (Africa joined in 2007):
  - different cultures, languages, traditions, also within the same country
- From different fields:
  - **30% from records and archives disciplines/professions** (among them 25% academics and 75% professionals)
  - **10% from IT, computer science and engineering**
  - **60% were records creators**: from business (e.g. pharmaceutical and chemical industry), arts (e.g. music, dance), sciences (e.g. physics), etc.

We had to agree on the basics for research and communication purposes: what is a record and how we recognize it; what is an authentic record.

InterPARES Trust

Basic Concepts

Based on Jenkinson:

- A **record** – or **archival document** – is any document made or received in the course of activity, and kept for further action or reference (i.e. created)
  - Being a document (i.e. information affixed to a medium), a record has stable content and fixed form
- Because of the circumstances of its creation a record is **natural**, (a by-product of activity), **interrelated** (linked by an archival bond) **impartial** (not created to answer questions researchers may ask of it in the future), and **authentic** (with respect to the creator, if used as an instrument of activity)

To **preserve** a record means to ensure its physical and/or technological stabilization (for the purpose of extending its life indefinitely) and the protection of its intellectual content and relationships

- Digital preservation is the process of maintaining digital materials authentic and accessible during and across different generations of technology over time, irrespective of where they are stored

InterPARES Trust

Did These Concepts Work?

- Like a charm! Why?
- By making archival document and record coincide we were able to move archival preservation (and other archival functions linked to it, such as appraisal – pretty much as Jenkinson wanted) up **to the time of creation**
- They were robust enough to allow us not only to distinguish records from other digital entities—and find ways of protecting their ability to serve as evidence, but also to identify a typology of digital records, from non-dynamic to interactive
- They enabled us to elaborate on the concepts of impartiality and authenticity and define the concept of **trustworthiness**

InterPARES Trust

Trustworthiness

Reliability

The trustworthiness of a record as a **statement of fact**,

based on:

- the competence of its author
- the controls on its creation

Accuracy

The **correctness and precision** of a record's data

based on:

- the competence of its author
- the controls on content recording and transmission

Authenticity

The trustworthiness of a record that **is what it purports to be**, untampered with and uncorrupted

based on:

- identity
- integrity

InterPARES Trust

Identity

Identity 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 creation (i.e., author, addressee, writer, originator, creator);
- its **date(s)** of creation (i.e. making, receipt, filing) and transmission;
- the matter or **action** in which it participates;
- the expression of its **relationships** with other records (e.g. classification code); and
- an indication of any **attachment(s)**

InterPARES Trust

Integrity

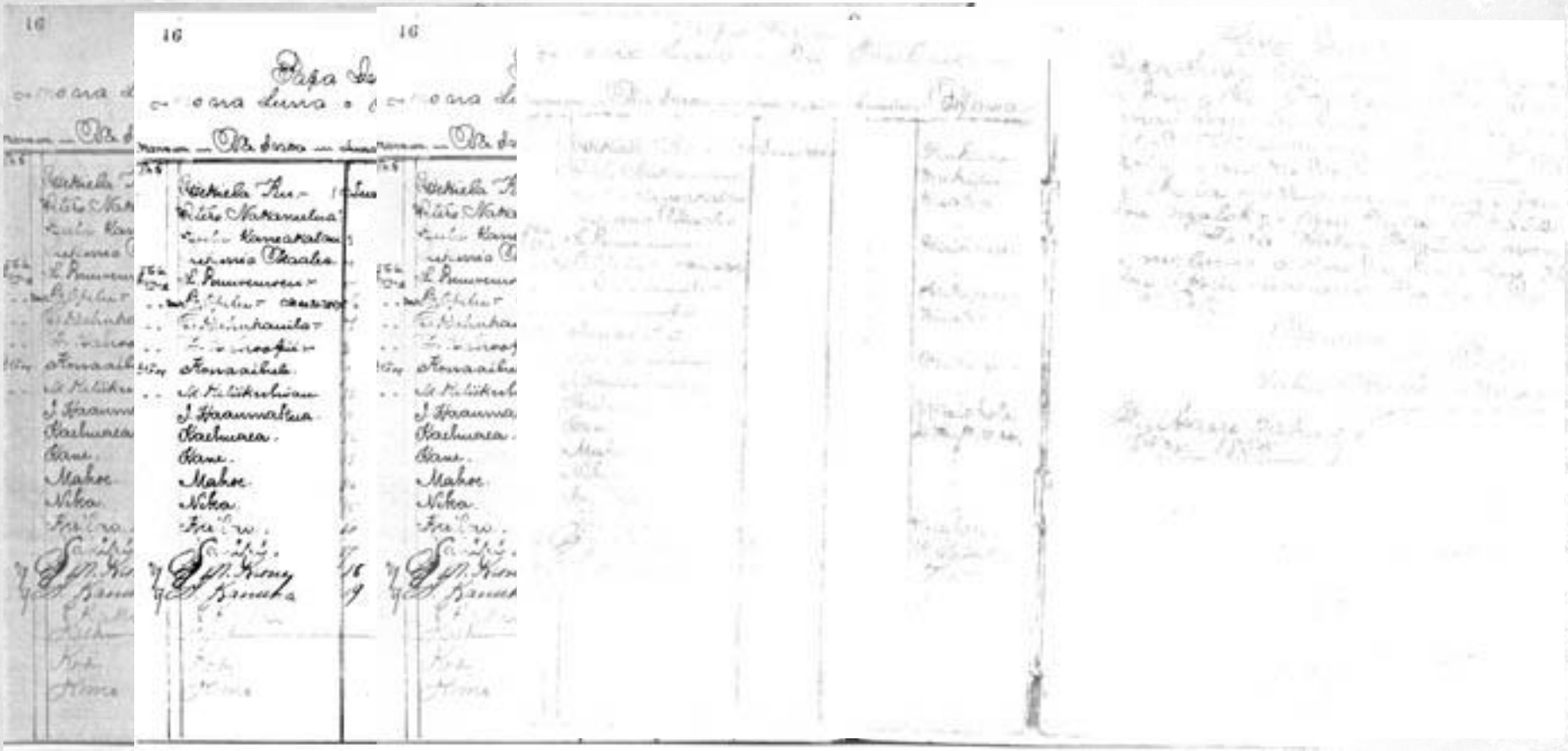
Integrity refers to the quality of being complete and unaltered in all essential respects.

We were never fussy about it. What if a document had holes, was burned on a side or the ink passed through?

The same definition of integrity was used with respect to data, documents, records, copies, records systems

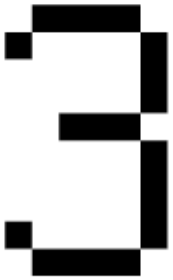
As long as it was good enough to understand it, ...but how good is good enough in the digital environment?

Loss of Integrity: Analog Document



Loss of Integrity: Digital Document

- If Original Bits 101
- Change state to 110
- Continues to a 011



- Same bits, but

  Different value

InterPARES Trust

Bitwise Integrity

Often identified with **Data Integrity**:

- The data in the document are not modified either intentionally or accidentally
- The original **bits are in a complete and unaltered state** from the time of capture, that is, they have the exact and same order and value

A small change in a bit means a very different value presented on the screen or action taken in a program or database.

Duplication Integrity

The process of creating a copy does not modify a record (either intentionally or accidentally) as the output is an exact bit copy of the original data set (form, content and composition data).

Duplication integrity is **linked to time** and one should consider the use of time stamps for that purpose.

But, in the digital environment, when we say duplication, we need to be explicit about what we mean, copy or image?

InterPARES Trust

Duplication: Copy

Selective duplicate (e.g. PDF)

- You only copy what you see
- Rarely includes confirmation of completeness
- Provides incomplete picture of the digital environment

Duplication: Image

Forensic duplicate:

A bit by bit reproduction of the storage medium and its content, including ambient data (e.g. snapshots of each open file), swap space (virtual memory, with passwords and encryption keys) and slack space (with deleted material)

Duplication Process Integrity: Principles

Principle of Non-interference: the method used to re-produce or re-create a digital document does not change the digital entities

Principle of Identifiable interference: if the method used does alter the entities, the changes are identifiable and identified (including para-data)

Authentication

Definition: A declaration of authenticity based on either direct knowledge, material proof, inference, or deduction

Basis for authentication of digital records

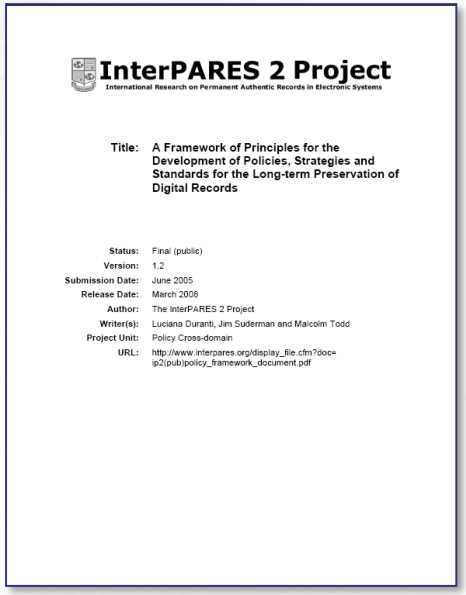
- **A chain of legitimate custody** remains ground (an increasingly significant ground!) for inferring authenticity and authenticate a record (**Jenkinson!** unbroken chain of custody).
- **Digital chain of custody:** the information preserved about the record and its changes that shows specific data was in a particular state at a given date and time.
- A **declaration** made by an expert who bases it on the trustworthiness of the system hosting the record and procedures and processes controlling its preservation and use

InterPARES Trust

IP 1 & 2 Products

Policy Framework

A framework of principles guiding the development of policies for records creating and preserving organizations



InterPARES 2 Project
International Research on Permanent Authentic Records in Electronic Systems

Title: A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records

Status:	Final (public)
Version:	1.2
Submission Date:	June 2005
Release Date:	March 2008
Author:	The InterPARES 2 Project
Writer(s):	Luciana Duranti, Jim Suderman and Malcolm Todd
Project Unit:	Policy Cross-domain
URL:	http://www.interpares.org/display_file.cfm?doc=ip2(pub)policy_framework_document.pdf

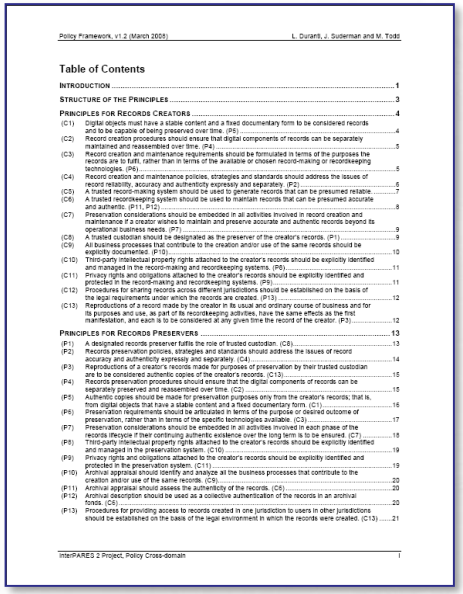


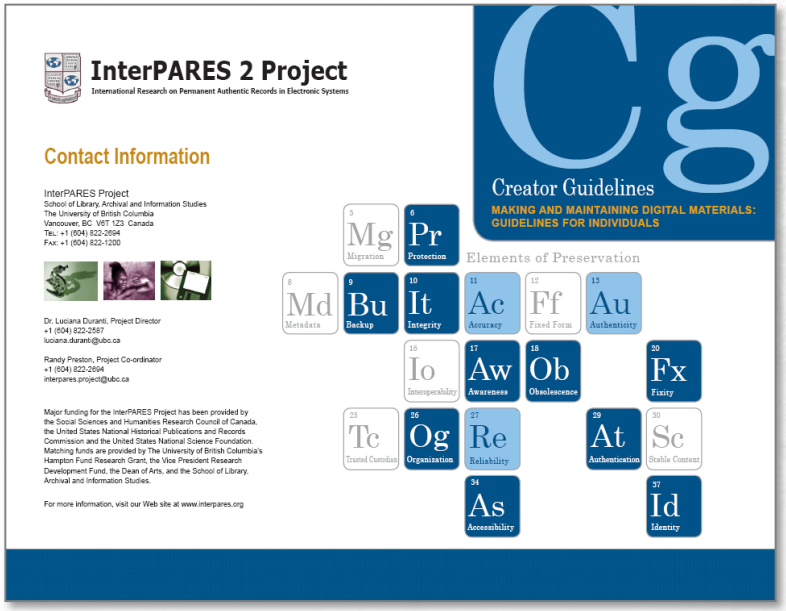
Table of Contents

InterPARES Trust

IP 1 & 2 Products

Creator Guidelines

Recommendations for making and maintaining digital materials for individuals and small communities of practice

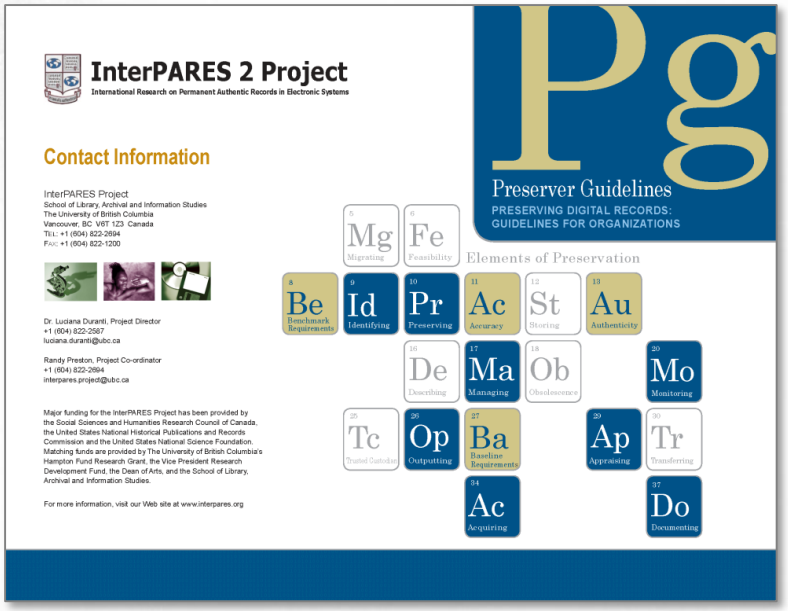


InterPARES Trust

IP 1 & 2 Products

Preserver Guidelines

Recommendations for digital preservation for archival institutions

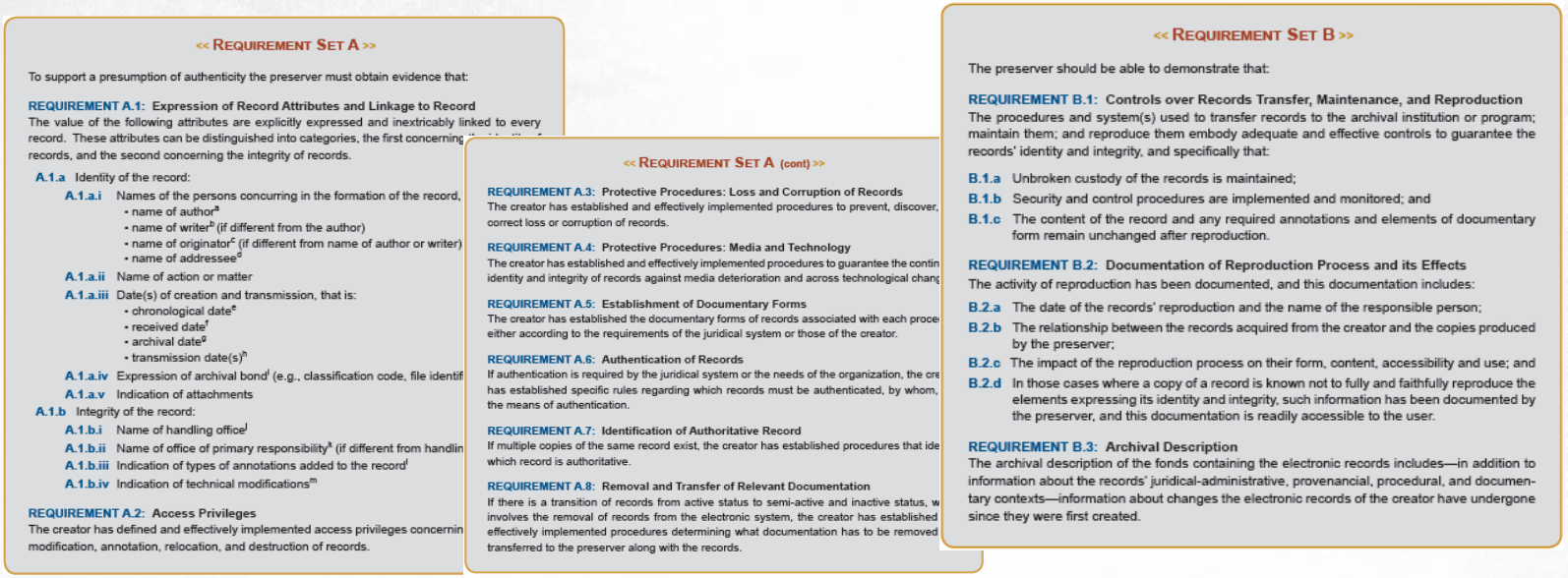


InterPARES Trust

IP 1 & 2 Products

Benchmark and Baseline Authenticity Requirements

Requirements for assessing and maintaining the authenticity of digital records



<< REQUIREMENT SET A >>

To support a presumption of authenticity the preserver must obtain evidence that:

REQUIREMENT A.1: Expression of Record Attributes and Linkage to Record
The value of the following attributes are explicitly expressed and inextricably linked to every record. These attributes can be distinguished into categories, the first concerning
records, and the second concerning the integrity of records.

A.1.a Identity of the record:
- A.1.a.i Names of the persons concurring in the formation of the record,
  - name of author[a]
  - name of writer[b] (if different from the author)
  - name of originator[c] (if different from name of author or writer)
  - name of addressee[d]
- A.1.a.ii Name of action or matter
- A.1.a.iii Date(s) of creation and transmission, that is:
  - chronological date[e]
  - received date[f]
  - archival date[g]
  - transmission date(s)[h]
- A.1.a.iv Expression of archival bond[i] (e.g., classification code, file identif
- A.1.a.v Indication of attachments

A.1.b Integrity of the record:
- A.1.b.i Name of handling office[j]
- A.1.b.ii Name of office of primary responsibility[k] (if different from handlin
- A.1.b.iii Indication of types of annotations added to the record[l]
- A.1.b.iv Indication of technical modifications[m]

REQUIREMENT A.2: Access Privileges
The creator has defined and effectively implemented access privileges concernin
modification, annotation, relocation, and destruction of records.

<< REQUIREMENT SET A (cont) >>

REQUIREMENT A.3: Protective Procedures: Loss and Corruption of Records
The creator has established and effectively implemented procedures to prevent, discover,
correct loss or corruption of records.

REQUIREMENT A.4: Protective Procedures: Media and Technology
The creator has established and effectively implemented procedures to guarantee the contin
identity and integrity of records against media deterioration and across technological chang

REQUIREMENT A.5: Establishment of Documentary Forms
The creator has established the documentary forms of records associated with each proce
either according to the requirements of the juridical system or those of the creator.

REQUIREMENT A.6: Authentication of Records
If authentication is required by the juridical system or the needs of the organization, the cre
has established specific rules regarding which records must be authenticated, by whom,
the means of authentication.

REQUIREMENT A.7: Identification of Authoritative Record
If multiple copies of the same record exist, the creator has established procedures that ide
which record is authoritative.

REQUIREMENT A.8: Removal and Transfer of Relevant Documentation
If there is a transition of records from active status to semi-active and inactive status, w
involves the removal of records from the electronic system, the creator has established
effectively implemented procedures determining what documentation has to be removed
transferred to the preserver along with the records.

<< REQUIREMENT SET B >>

The preserver should be able to demonstrate that:

REQUIREMENT B.1: Controls over Records Transfer, Maintenance, and Reproduction
The procedures and system(s) used to transfer records to the archival institution or program; maintain them; and reproduce them embody adequate and effective controls to guarantee the records' identity and integrity, and specifically that:

- B.1.a Unbroken custody of the records is maintained;
- B.1.b Security and control procedures are implemented and monitored; and
- B.1.c The content of the record and any required annotations and elements of documentary form remain unchanged after reproduction.

REQUIREMENT B.2: Documentation of Reproduction Process and its Effects
The activity of reproduction has been documented, and this documentation includes:

- B.2.a The date of the records' reproduction and the name of the responsible person;
- B.2.b The relationship between the records acquired from the creator and the copies produced by the preserver;
- B.2.c The impact of the reproduction process on their form, content, accessibility and use; and
- B.2.d In those cases where a copy of a record is known not to fully and faithfully reproduce the elements expressing its identity and integrity, such information has been documented by the preserver, and this documentation is readily accessible to the user.

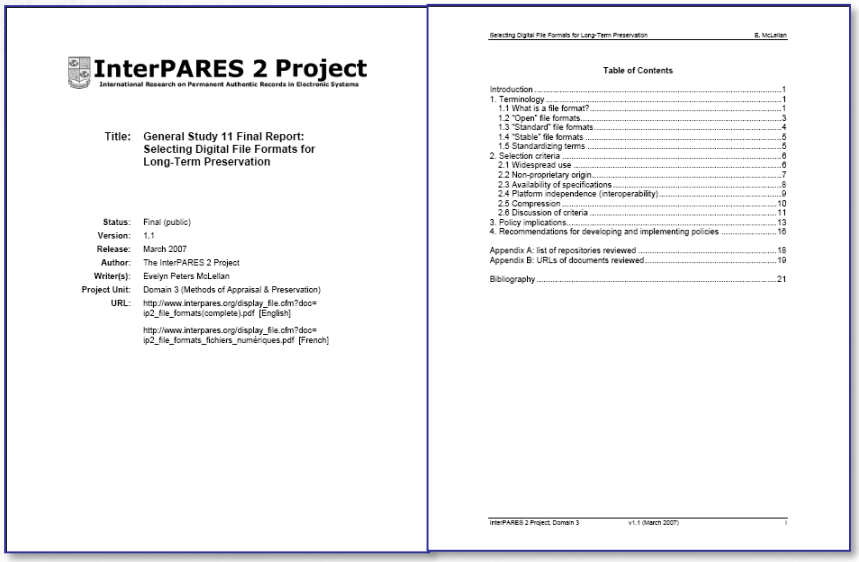
REQUIREMENT B.3: Archival Description
The archival description of the fonds containing the electronic records includes—in addition to information about the records' juridical-administrative, provenancial, procedural, and documentary contexts—information about changes the electronic records of the creator have undergone since they were first created.

InterPARES Trust

IP 1 & 2 Products

File Format Selection Guidelines

Principles and criteria for adoption of file formats, wrappers and encoding schemes



InterPARES 2 Project
International Research on Permanent Authentic Records in Electronic Systems

Title: General Study 11 Final Report: Selecting Digital File Formats for Long-Term Preservation

Status: Final (public)
Version: 1.1
Release: March 2007
Author: The InterPARES 2 Project
Writer(s): Evelyn Peters McLellan
Project Unit: Domain 3 (Methods of Appraisal & Preservation)
URL: http://www.interpares.org/display_file.cfm?doc=ip2_file_formats(complete).pdf [English]

http://www.interpares.org/display_file.cfm?doc=ip2_file_formats_fichiers_numériques.pdf [French]

Selecting Digital File Formats for Long-Term Preservation — E. McLellan

Table of Contents

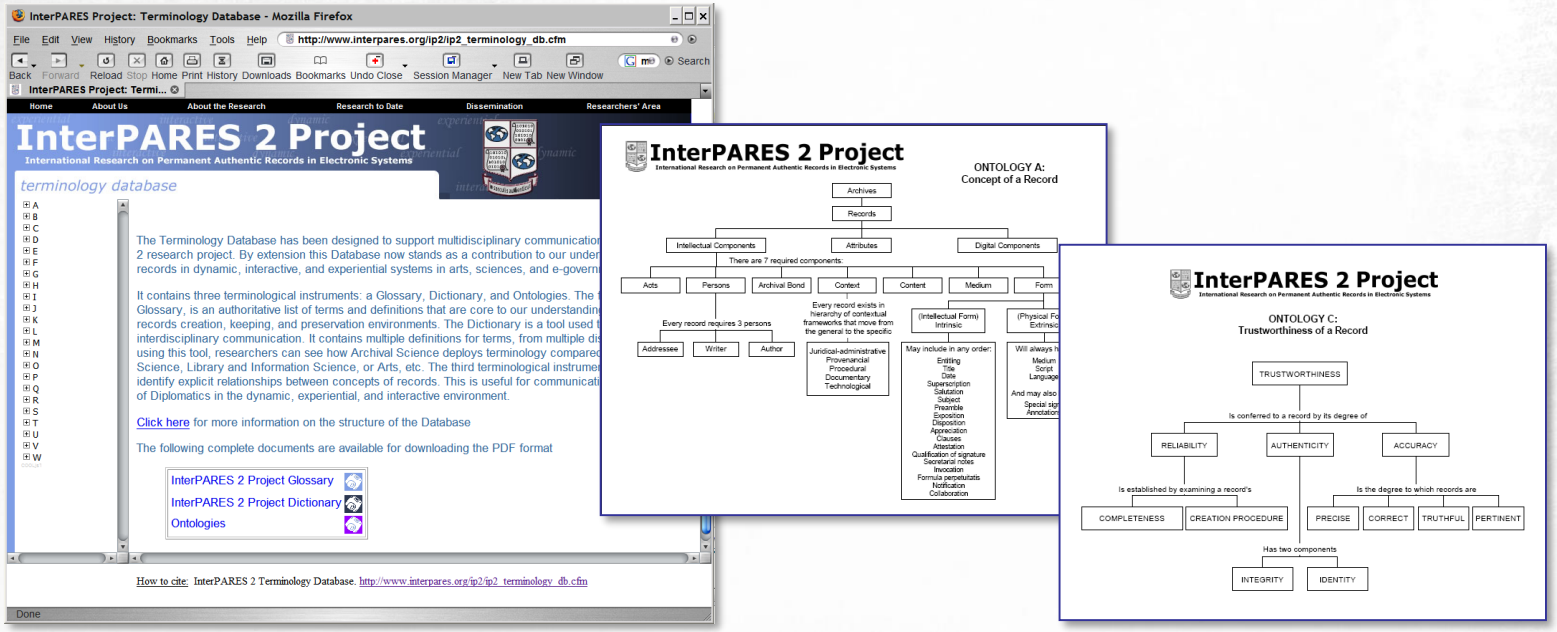
InterPARES 2 Project, Domain 3 — v1.1 (March 2007) — i

InterPARES Trust

IP 1 & 2 Products

Terminology Database

Including a glossary, a dictionary and ontologies. The glossary became the ICA Multilanguage Terminology Database

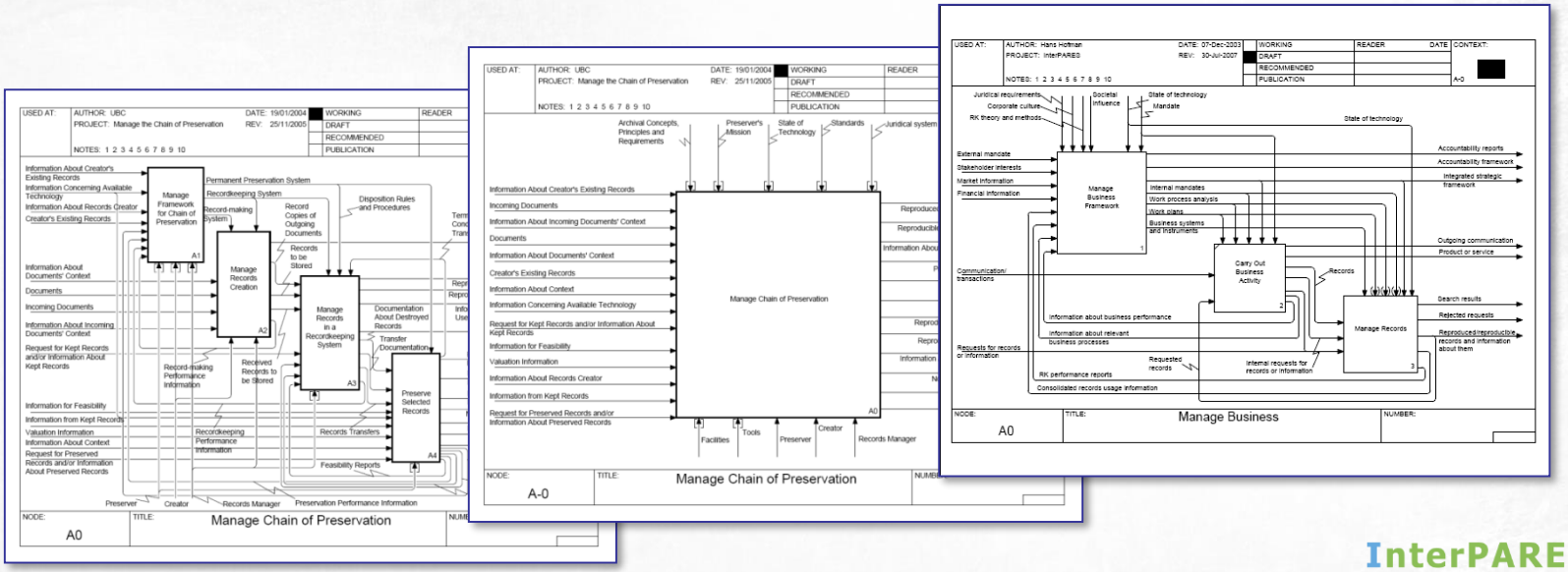


InterPARES Trust

IP 1 & 2 Products

Two Records Management Models

Chain of Preservation (COP) Model (lifecycle)
Business-driven Recordkeeping (BDR) Model (continuum)



InterPARES Trust

IP 1 & 2 Final Products

Two books:

Luciana Duranti, ed. *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project* (San Miniato: Archilab, 2005). Available on line at http://www.interpares.org/book/index.cfm

Luciana Duranti and Randy Preston, eds. *InterPARES 2: Interactive, Dynamic and Experiential Records* (Roma: ANAI, 2008). Available on line at http://www.interpares.org/ip2/book.cfm.

Goal of InterPARES 3 (2007-2012)

To **enable** public and private **archival organizations and programs** with limited resources **to preserve** over the long term **authentic records** that satisfy the requirements of their stakeholders and society's needs for an adequate record of its past.

It did so by building on the products of the first two phases of InterPARES 1 & 2

Some InterPARES 3 Studies

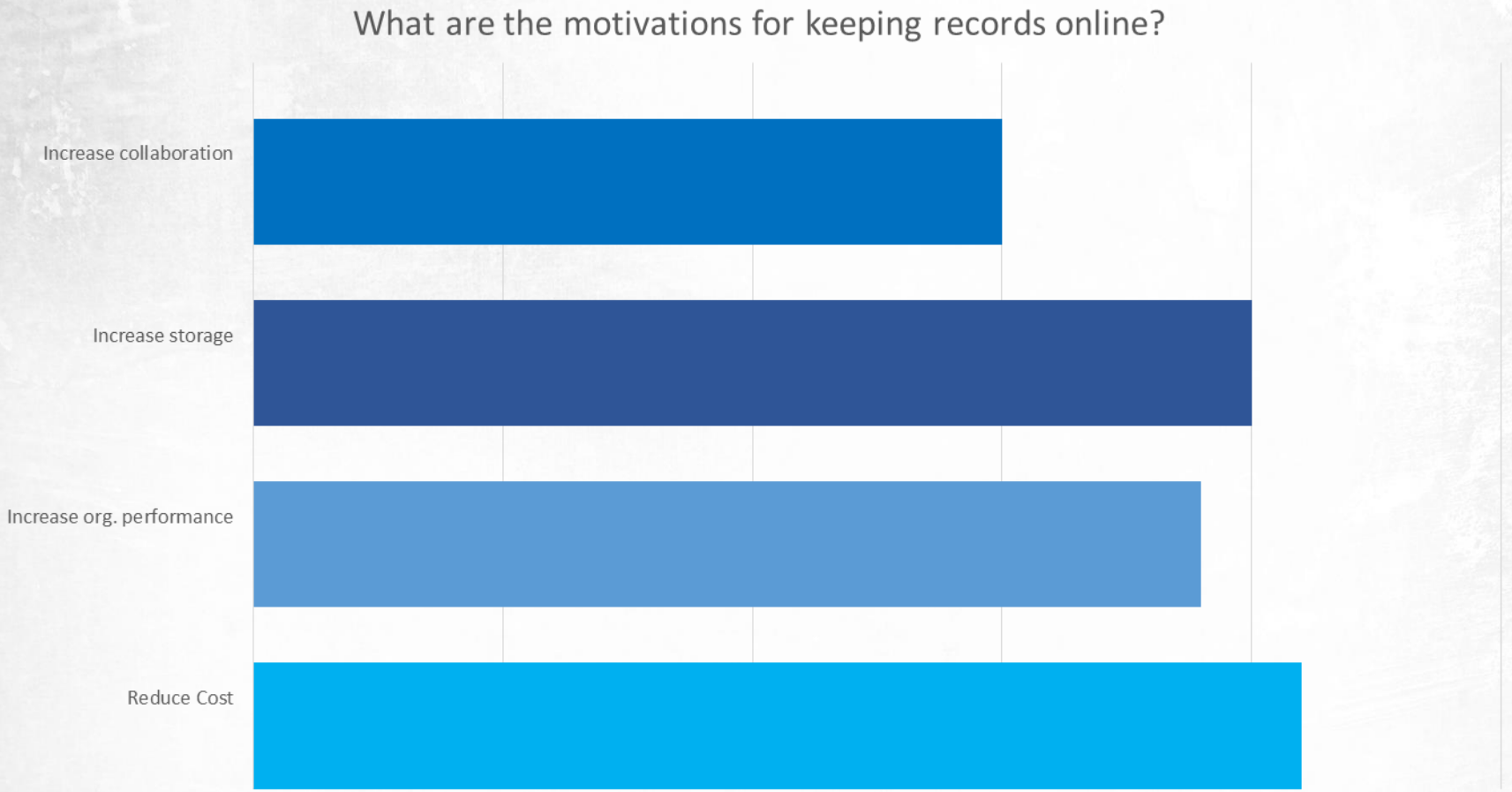
- Community Archives e-Records Assessment
- Public Sector Audit Report for Digital Recordkeeping
- Open Source Records Management Software
- **Metadata Applications Profiles**
- Organizational Culture & Risk Assessment
- **E-mail Preservation**
- Preservation of Registries
- Education Modules on Digital Preservation

InterPARES Impact

- Legislation: Italy, China
- Standards: DOD 5015.2 (2007), MoReq 2 (2008), OAIS (2009), ARMA (e.g. electronic messages 2012 & 2018), CGSB (72-34: 2005 and 2017), ISO 30300 series
- Policies and Procedures: participating countries in both public and private sectors
- ICA Education Modules and Multilingual Archival Database

All InterPARES products are available at www.interpares.org

Records in the Cloud



InterPARES Trust

InterPARES Trust (2013-2019)

The **goal of InterPARES Trust** is to generate the theoretical and methodological **frameworks** that will support the development of **integrated** and **consistent** local, national and international **networks of policies, procedures, regulations, standards and legislation concerning digital records entrusted to the Internet**, to ensure public trust grounded on evidence of good governance, a strong digital economy, and a persistent digital memory.

Issues

- Data ownership
- Availability, access, and reliability
- Retention and disposition
- Storage and maintenance
- Security
- Location and transfer
- End of service
- Preservation
- Users Behaviour
- Trustworthiness

Data Ownership

- When a user entrusts its records to a provider and uses the latter's platform and application to generate additional data, the **provider will create data** related to actions about data processing, management, etc.
- While the content created and/or stored in the cloud by the user is owned by such user, **the metadata created by the provider are not**, and, as the user needs them to demonstrate the integrity of the records, contractual agreements should determine whether and how the user has the **right to access and use the provider's metadata**.

Availability, Access, Reliability

- **Availability** is a fact, while **access** is a right, but the latter cannot be satisfied without the former
- In a cloud environment, **availability of the stored records** implies also the **availability of the infrastructure** (i.e. the amount of time that a system is expected to be in service is 100%), which facilitates the retrieval and readability of the data, because technical difficulties might slow a FOIA process and the owner of the data, being liable for providing access to them, may be sanctioned
- **Reliability** is the characteristic of behaving consistently with expectations: one must consider not only availability of the records through redundancy but also **consistency** and **accuracy** of access.

Records Retention and Disposition

- **Compliance** is difficult to verify.
  - **transfer** from a system to another for retention might involve loss of authenticity
  - **destruction** might involve
    - a breach of confidentiality or privacy,
    - persistence of some of the copies and related metadata, and
    - persistence of the metadata generated by the provider about the user's data.

Records Storage and Maintenance

- Storage and maintenance impact the quality of the records and they ability to serve as legal evidence, especially in legal jurisdictions where the **authenticity** of the record is an inference made from the **integrity** of the system where the data reside (Canadian Government Standard Board 74:32 2017).
- Contractual agreements do not generally specify how records are maintained **across changing technologies and data formats**, and they generally say that users are responsible for backing up their data. All maintenance procedures, including proper storage, care, custody, and data control, are referred to by providers as “backup procedures.”

InterPARES Trust

Records Security

- It is protection of the system/records from **unauthorised access, use, alteration or destruction.** In a world where integrity of a system is an inference from which one infers integrity of the record, from which one infers its authenticity and then trustworthiness, **security is the new authenticity**.
- Individuals enforce security with something they know (e.g. password), they own (e.g. tokens), or they are (e.g., biometrics of eyes, fingerprints, private keys in a PKI environment)
- A cloud provider enforces it through encryption and should **produce audit trails and access logs** and capture, maintain and make available **metadata** associated with access, retrieval, use and management of the data, in addition to those linked to the data themselves.
- **The security issue links directly to the matter of data location and cross-border data flow.**

InterPARES Trust

Records Location and Transfer

- The cloud is the platform of choice for **mobile applications** and the data generated using them, as well as those created in **smart devices.** Records can be in data centres anywhere in the world
- The location of the records is a criterion in **determining the law that applies** in case of litigation
- National strategies used to require that records resides within the boundaries of the country where they were created (very expensive for data centres, if Europe or North America).
- The international strategy no longer requires that, thereby underscoring the importance of **multilateral agreements** among countries for collaboration in security (new safe harbour)

InterPARES Trust

End of Service – Contract Termination

- If the provider ceases to exist or terminates one or more of its services (for breach, inactivity, or convenience), the records will be **deleted** or **inaccessible**
- Free services do not have an established duration and may close accounts **unilaterally**, requiring users to delete software and applications, and preventing them from accessing the data left with the provider
- When the data are given back to the user it is not certain that they will be in a **usable** and **interoperable** format
- If the contract is terminated by the user, the restitution of the data may be **expensive** and the data may not be in accessible formats. Also, the user may not have **the right to access the metadata** generated by the system for its recordkeeping or legal purposes, and may have no guarantee that the provider will **destroy** every copy of the data held in the data centers

InterPARES Trust

Records Preservation

- Preserving records in the cloud is a **black box process**
- Providers **may not know where the records are**, can and do **subcontract** some of their services to other providers, potentially maintaining servers or being registered as providers in different countries.
- One cannot expect that the same hardware and software will remain in service for as long as the records must be preserved, or that the technologies replacing them will be **compatible** with the previous ones.
- Standards give information about preservation formats but there is **no way of controlling compliance**

InterPARES Trust

Users Behaviour: Reuse

- Reuse is often ***remix***, which results in **derivative works** that may substantively change the intent and context of the appropriated material.
- Reuse involves **successive cycles of use, modification, repurposing,** and of course **take-down notices**.

User Behaviour: Sharing

- People **share profiles** for a variety of social media and web sites, and **post material** they consider informative.
- Social media platforms facilitate the movement of material **from one circle of people to another**.
- Groups assemble and change **stories of activities and events**.

Sharing (cont.)

- Dynamic groups of employees from public agencies collectively create a body of **interlinked material** related to a work project (e.g. gcpedia), a common interest, putting into question who owns it and what the context is.
- Contributions to social media by people, programs, committees, or agencies **now dead are linked to ongoing, active contributions** of the living, or disappear, or appear as created by their successors.
- **Digital lives, activities, initiatives are linked to each other.**

InterPARES Trust

User Behaviour: Control and Access

- Massive amounts of **data about individuals** in the cloud are controlled by corporations and governments (**big data)**
- **Medical records** including genotyping or gene sequencing data, medical history, prescription and insurance information, tests, and images are **held by the medical establishment in community clouds** which makes them accessible.
- **Genealogies**, factual biographies, biographic data and personal images available on the web **belong to the private platform hosting them** (Instagram, Facebook, Google).
- In addition to big data, open data and open government raise the issue of **traceability to and identification of the source records (lineage)**

InterPARES Trust

Technology Dependent Authentication

Digital signature:

- protects **bitwise integrity**
- verifies a record's origin (part of its **identity**), makes record indisputable and incontestable (**non-repudiation**)
- has been given legal value by legislative acts (e.g., European Directive on electronic signatures) or regulatory bodies (Security Exchange Commission on hash functions)
- is enabled through complex and costly public-key infrastructures (PKI)
- ensures authenticity of information **across space,** not **time**!
- is subject to **obsolescence**, and compounds the problem of preservation as it cannot be migrated with the record it is attached to, and the certificates have an expiration date
- Theory tells us that it has the function of a **seal**, rather than of a signature, so it can be removed and substituted with metadata

InterPARES Trust

Technology Dependent Authentication

Blockchain technology

- the underlying technology enabling Bitcoin
- a ledger, i.e. an information store which keeps a final and definitive (immutable) trace of transactions (their hash).

- relies upon a **distributed network** **(**all nodes—servers are equal) and **decentralized consensus** (no centre(s); no single point of control or attack)
- The confirmed and validated sets of transactions are held in blocks, which are linked (chained) in a chain that is tamper-resistant and append-only
- It starts with a genesis block and each block contains, in addition to the hash of a predetermined number of documents, a hash of the prior block in the chain.

InterPARES Trust

How is Blockchain used?

Blockchain can be used to confirm

- the **integrity** of a record kept elsewhere
- that a record **existed** or **was created** at a certain point in time (i.e. not after being timestamped and registered in the blockchain)
- the **sequence** of uploading of records to the blockchain

Is it a **recordkeeping system**? No. It holds the hash of records, not records, except for smart contracts (i.e. agreement between parties directly written into lines of code). The records must still be stored and managed off chain. This is good, because, if they were in the blockchain, they would be **immutable**, impossible to delete or reorganise.

InterPARES Trust

Legal Problems with Blockchain Authenticated Records

- Proving **reliability, accuracy** and **authenticity at origin** (impartiality and authenticity)
- Preserving the **archival bond** and contextual evidence (naturalness and interrelatedness)
- Handling the **decentralized** (and thus trans-jurisdictional) nature of the blockchain (who is the creator?)
- When the records result from **smart contracts**, dealing with code in a situation where the necessary components of a record are controlled by different actors in different jurisdictions. Plus, no required elements like a signature and the date of the completion of the agreement.

InterPARES Trust

Jenkinson Disrupted

- The record has disintegrated, pulverized, in a myriad data: if data are the new record, what about context? **Interrelatedness** among what?
- Trustworthiness is an inference and not verifiable: if security and immutability are the new trustworthiness, what about reliability, identity, and integrity? **Impartiality** and **authenticity** on the basis of what?
- Technological control is the new panacea: if the creator and the preserver delegate responsibility to technology and their providers, what about the usual and ordinary course of business? **Naturalness** of what?
- **Can the record as we knew it continue to exist?** Can legislation on the duty to document resurrect it? Should we even wish for it? Shouldn't we go our merry way trusting the "information" that "we feel like" trusting and dispense with the idea of the trustworthy record altogether?

InterPARES Trust

The InterPARES Reply

Context:

- ISO has embedded in its latest records management standard (2016) the most controversial of Jenkinson ideas, appraisal by the creator, and its appraisal technical report (2018) supports the idea that long term value to the creator coincides with historical value (as in the Grigg report and the Public Records Act of 1958)
- the information environment in which we operate agrees that preservation consists of protecting the nature of the record as intended by its creator (the moral defence of archives), as Jenkinson believed
- the need for the evidentiary capacity of information is made compelling and non renounceable by the misinformation and disinformation circulating in society: Jenkinson's sanctity of evidence

The InterPARES Reply

Conclusion:

The archival document, or record – natural, interrelated, impartial and authentic, together with the archives in which it belongs, must continue to form the **infrastructure through which beliefs and values are upheld and understood by society**.

We have no choice but to hold on to it!

Records/Archives in a Blockchain-based system

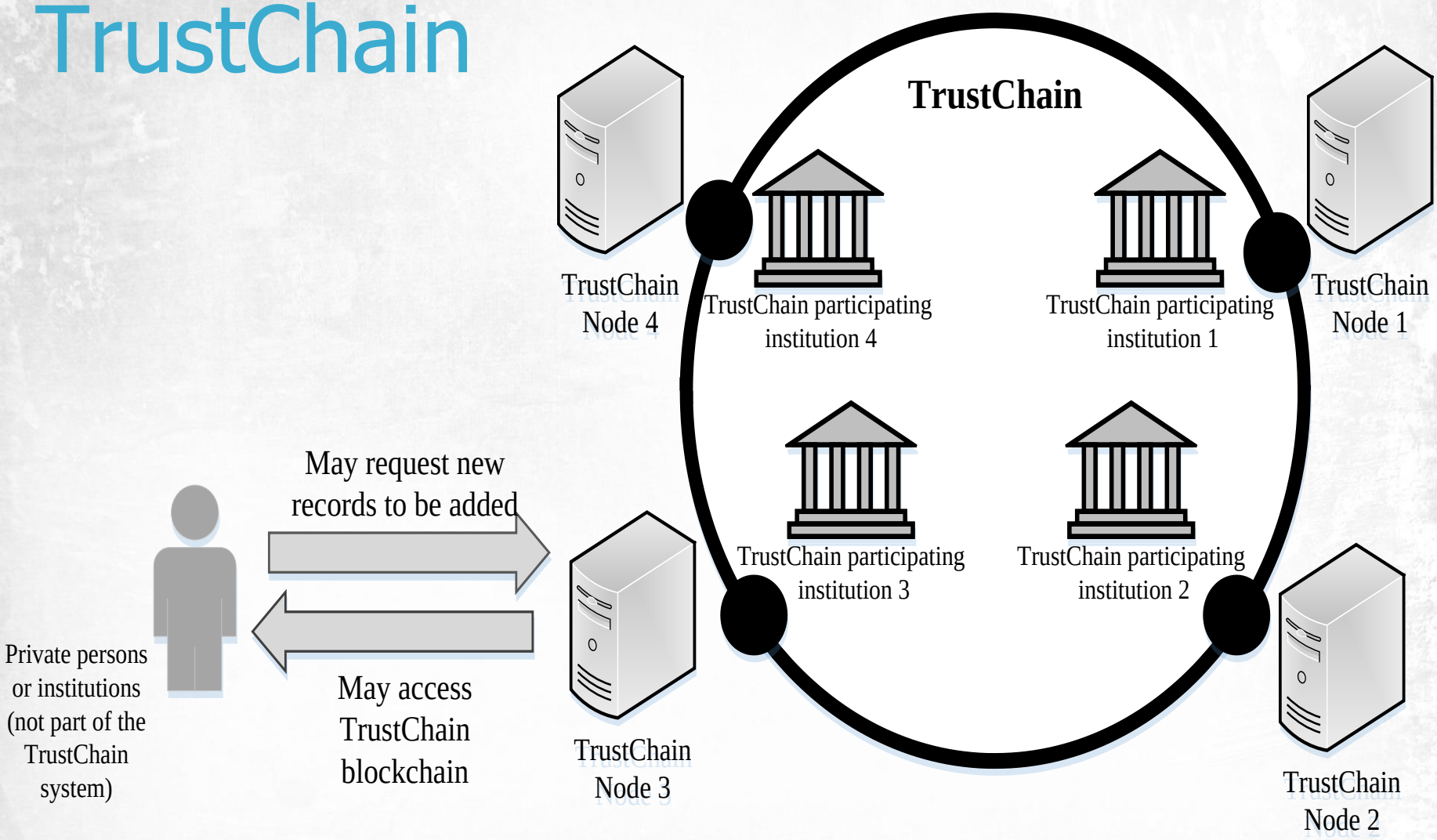
- InterPARES TRUSTER Preservation Model
  - Blockchain-based system called "**TrustChain**"
  - Applies the concepts of
    - hash algorythms
    - blockchain
    - distributed consensus
  - Presumptions:
    - private cloud blockchain
    - only approved nodes can write
    - everyone can read

TrustChain

The proposed **TrustChain** system

- relies on the involvement of a **group of trusted institutions**
- **the recordkeeping system in the creating office** and **the preservation system in the archives** would work **in concert** along the lifecycle of the records
- would provide confirmation of **integrity**, time of **creation/existence**, **sequence of records**, **non-repudiation**, **validity of e-signatures** whose certificate has not expired

TrustChain



InterPARES Trust

InterPARES Products Supporting Trustworthines

Security Classification:
https://interparestrust.org/assets/public/dissemination/TR03-Checklist-2_-final.pdf

Cloud Services Contracts:

https://interparestrust.org/assets/public/dissemination/NA14_20160226_CloudServiceProviderContracts_Checklist_Final.pdf

https://interparestrust.org/assets/public/dissemination/NA14_final_report_v5-1.pdf

Preservation as a Service for Trust:

https://interparestrust.org/assets/public/dissemination/PreservationasaServiceforTrust1_0-FINAL1.pdf

Jenkinson Disrupted?

The InterPARES research findings show that, far from being disrupted by emerging technologies, **Jenkinson's ideas are alive and well and more useful in the digital environment than they ever were in the analogue one.**

www.interparestrust.org

THANK YOU

luciana.duranti@ubc.ca

InterPARES Trust