InterPARES Trust

Design Requirements for Authenticity Metadata

Second International Symposium

Corinne Rogers, University of British Columbia
Joseph Tennis, University of Washington

Victoria, BC

October 17, 2014

outline

- introduction & background
- ‘ideal’ set of metadata for our purpose
- minimal set of metadata for our purpose
- theory vs practice – metadata in the field
- related ITrust studies – next steps
- conclusion

introduction

NA16 – metadata design requirements for authenticity in the cloud and across contexts:

- relationship between metadata, documentation, policies to support recordkeeping
- building on Benchmark Requirements Supporting Presumption of Authenticity & Baseline Requirements Supporting Production of Authentic Copies (IP 1 & 2)
- Chain of Preservation Model (IP 2)
- IP Authenticity Metadata Application Profile (IP 3)

background: premise

- authenticity of digital records is presumed with establishment of identity & demonstration of integrity
- realized through metadata & documentation that accrues throughout the lifecycle of records & data
- metadata reveals context and makes explicit how a system implements certain policies

background; what metadata do we need, when, and for what purpose?

"When it comes to declaring electronic records, information governance professionals have been struggling for some time with the issue of what metadata to preserve."

Isaza (2010) Metadata in Court, ARMA International

background: who's concerned about metadata?

- governments & commercial entities
  - service delivery; security monitoring; analytics; profit
- critics of both
  - privacy, civil rights
- archivists
  - preservation, authenticity, management
- digital forensics specialists
  - audit; security; incident response
- lawyers
  - ethical issues; discovery; admissibility

questions

- what is the ‘ideal’ set of metadata that will allow a presumption of authenticity throughout the lifecycle of digital objects?
- can we identify a minimum set of metadata required for an assessment of authenticity?
- what is the relationship between metadata and external forms of description and documentation?

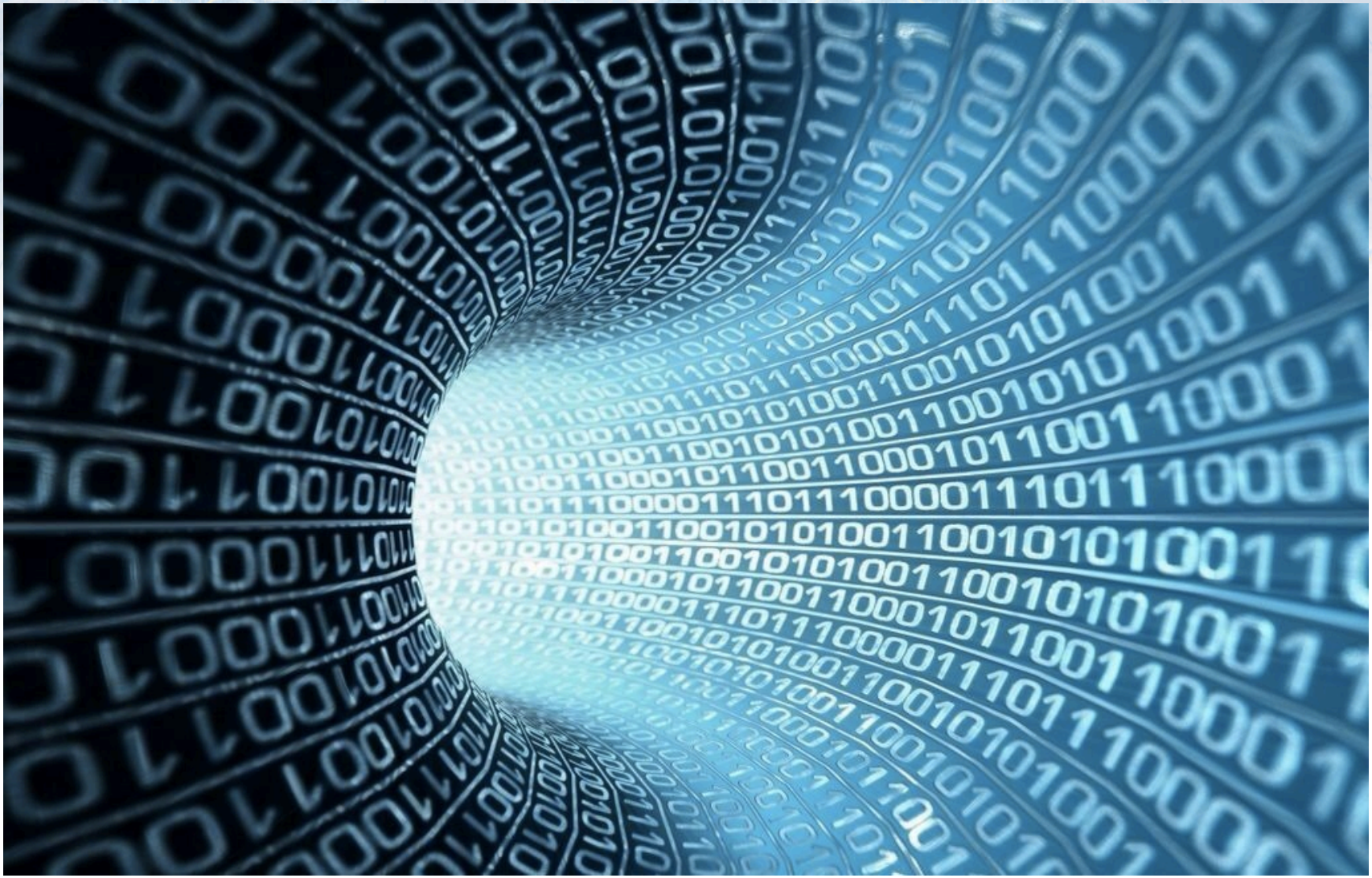
questions

- does the advent of cloud infrastructures change requirements for metadata necessary to assess authenticity?
  - does the use of a third party (CSP) introduce new metadata that affects our ability to assess authenticity

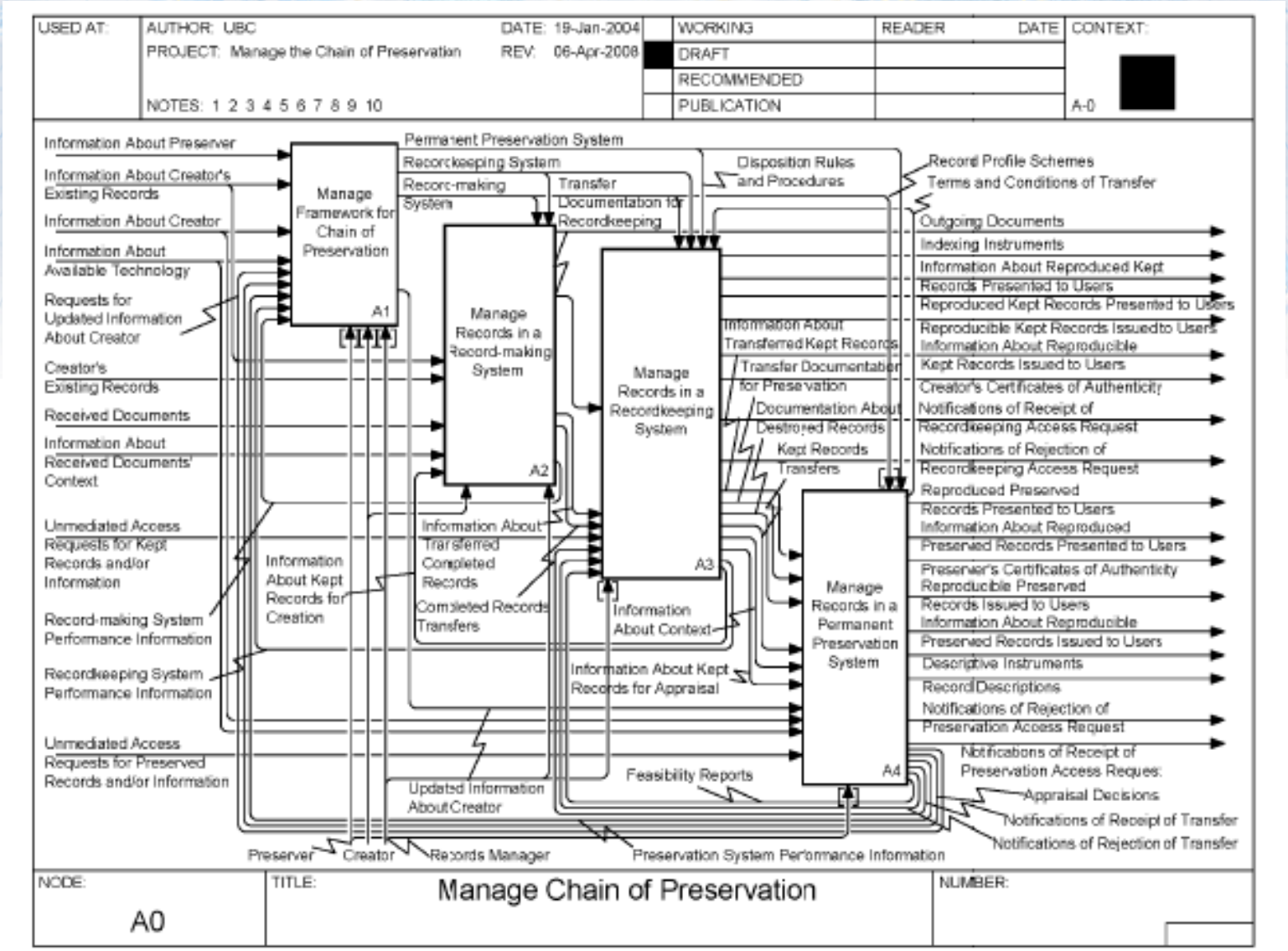
metadata risks in cloud computing

- insufficient metadata for chosen purpose
- fixity of metadata unclear
- unclear ability to retain metadata when downloading from the cloud
- loss of chain of custody because of CSP actions
- metadata applied by CSP may be relevant for assessment of controls on records but unavailable to us

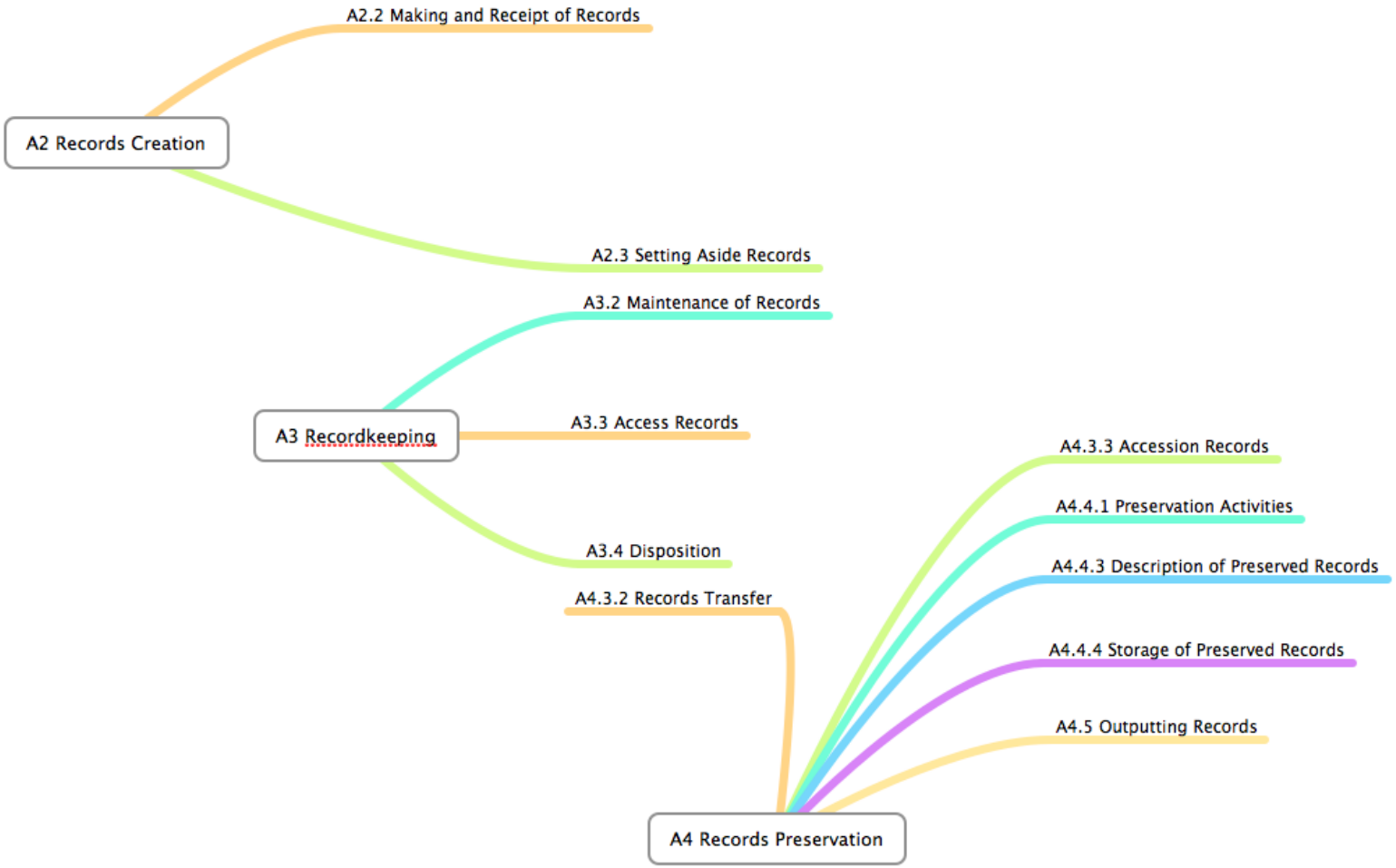
more than what meets the eye…



function & purpose: an ideal level of metadata?



visualization



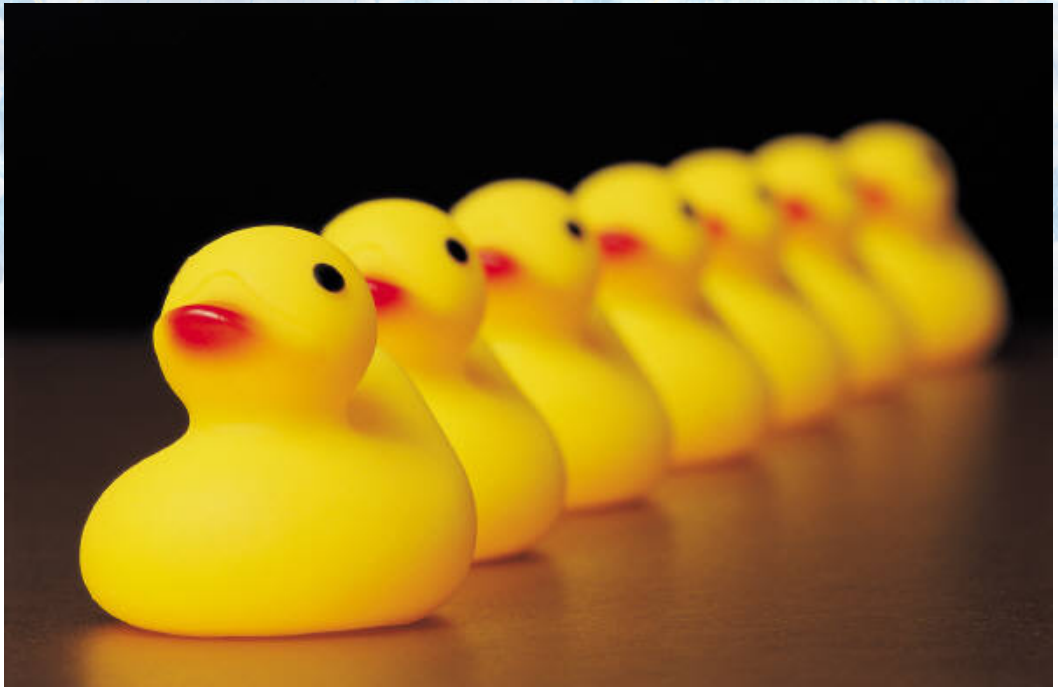
areas of description & metadata elements

identity
- P-persons
- D-date
- S-subject (action or matter)
- B-bond
- A-attachment

integrity
- T-technology
- F-form
- SS-seals & signs
- AU-authentication (inc digital sig, attestation etc
- R-rights and access; H-handling (office)

context
- DO-external documentation and system metadata (policy, context, appraisal, transfer, audits of system activity, requests on the records)

minimal set of metadata?



metadata in the field

- reliance on system
- reliance on their consistent practices

metadata in the field

- reliance on system
- reliance on their consistent practices
- reliance on procedure & policy

metadata in the field

- reliance on system
- reliance on their consistent practices
- reliance on procedure & policy
- reliance on system controls, e.g. audit trails
- revealed in metadata and documentation

metadata in the field

- reliance on system
- reliance on their consistent practices
- reliance on procedure & policy
- reliance on system controls, e.g. audit trails
- revealed in metadata and documentation

new developments

archivematica®

links to other ITrust projects

- PaaST – Preservation as a Service for Trust
  - chain of custody
  - chain of preservation
  - OAIS
- PaaST Archival Authentication Services
  - set benchmark assessment of authenticity at submission
  - apply archival authentication methods against an archival object or copy through preservation & access

standard of practice

- Standard of Practice for Trust in Protection of Authoritative Records
- risk management decisions
- global consensus to create a standard of practice for risk management in authoritative archives

conclusion

thank you!

www.interparestrust.org

cmrogers@mail.ubc.ca