InterPARES Trust

Authenticity as a Component of Information Assurance and Security

Corinne Rogers
University of British Columbia

ICCSM 2014
Reading, U.K.
October 23-24, 2014

trust, authenticity

- authentic: “of undisputed origin, genuine; reliable, trustworthy” *Canadian Oxford Dictionary s.v. ”authentic”*
- authenticity: “the quality of being authentic, or entitled to acceptance” *Oxford English Dictionary, 2nd ed., s.v. “authenticity”*
- reliable: “of sound and consistent character or quality” *Canadian Oxford Dictionary s.v. “reliable”*
- authentic record: a record that is what it purports to be and is free from tampering or corruption

  InterPARES 1, Authenticity Task Force

trust, authenticity, security

- authenticity frequently cited as an outcome or a goal of information assurance & security
  - protecting systems from unauthorized access
  - guaranteeing and protecting the contents of those systems – the records, documents, data, metadata – from theft, alteration, or deletion, and assuring their identity and integrity
- not about technology alone

terminology – archival science vs IAS

- lack of consistency of definitions of the objects and goals of IAS; between IAS and archival diplomatics
- example: record, integrity

assessing authenticity

- traditionally understood as deriving from circumstances of creation or place of preservation
- chain of custody
- presence of signatures
- testimony

problems of assessing authenticity of digital records

- authentication necessary in court – based on observation and testimony
- traditional heuristics not adequate in digital environment
- further complicated in a cloud environment

archival diplomatic theory

- links assessment of authenticity to the circumstances of record creation and framework of subsequent preservation
- establish identity and demonstrate integrity
- Chain of Preservation (CoP) model of authentic digital records in records systems

archival diplomatic theory

- 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 policies

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

background: who's concerned about metadata?

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

information assurance & security – a multi-disciplinary knowledge domain

- Information security: the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability
- information assurance: measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation *(NIST)*

compatibility of archival lifecycle models & IAS models

- metadata application profile for authenticity – archival diplomatic theory from CoP
- security goals of RMIAS – confidentiality, , integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability *(Cherdantseva & Hilton)*
- four quadrants: security development life cycle; information taxonomy; security countermeasures; security goals

metadata for authenticity

metadata elements required for assessment of authenticity:

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

integrity
- T-technological context
- 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) (*InterPARES – IPAM)*

areas of description & metadata elements

metadata elements required for assessment of authenticity:

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

integrity
- T-technological context
- 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) (*InterPARES – IPAM)*

security goals:

accountability

availability

authenticity/trustworthiness

auditability

confidentiality

integrity

non-repudiation

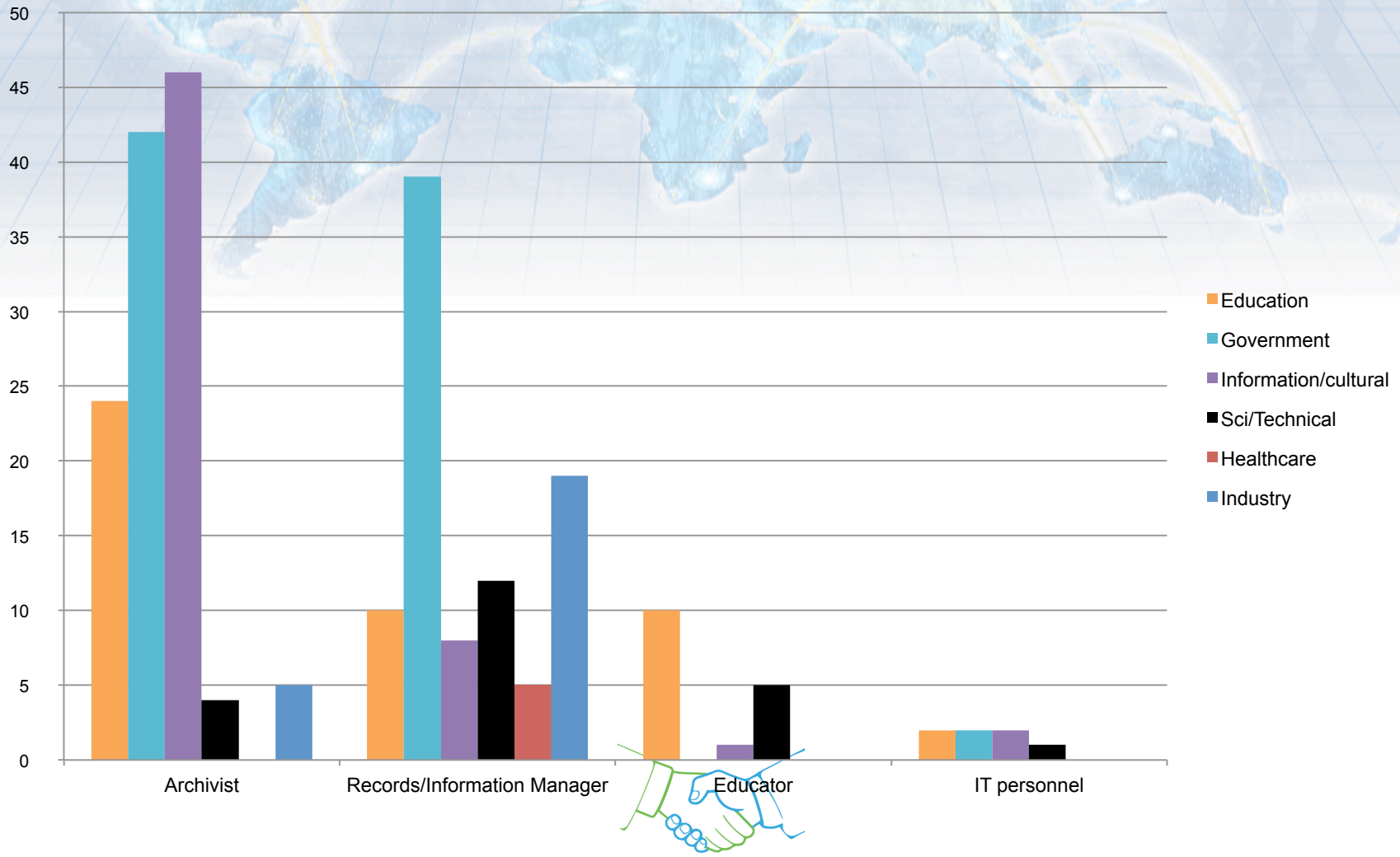
privacy

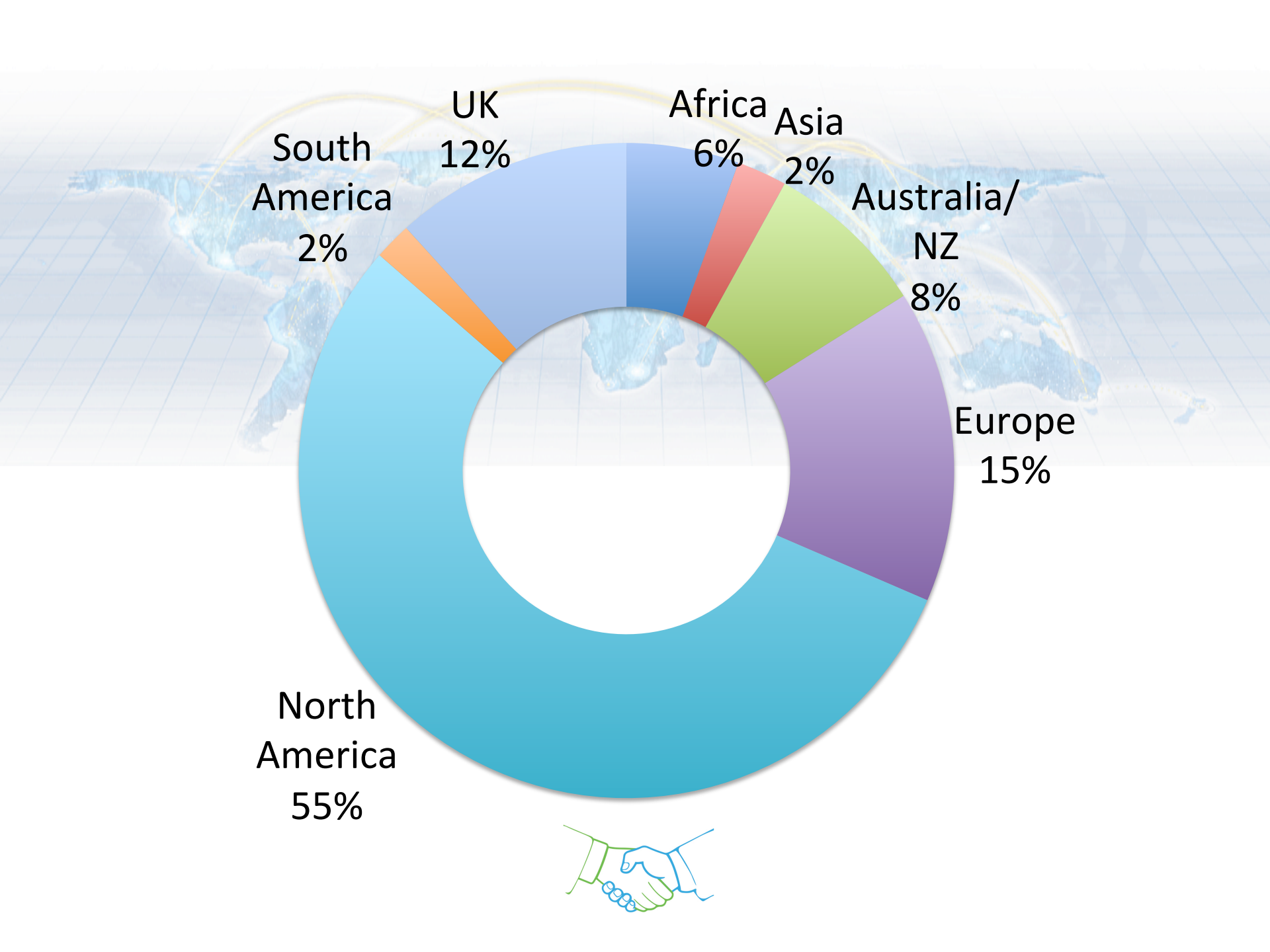
Cherdantseva & Hilton

theory & practice

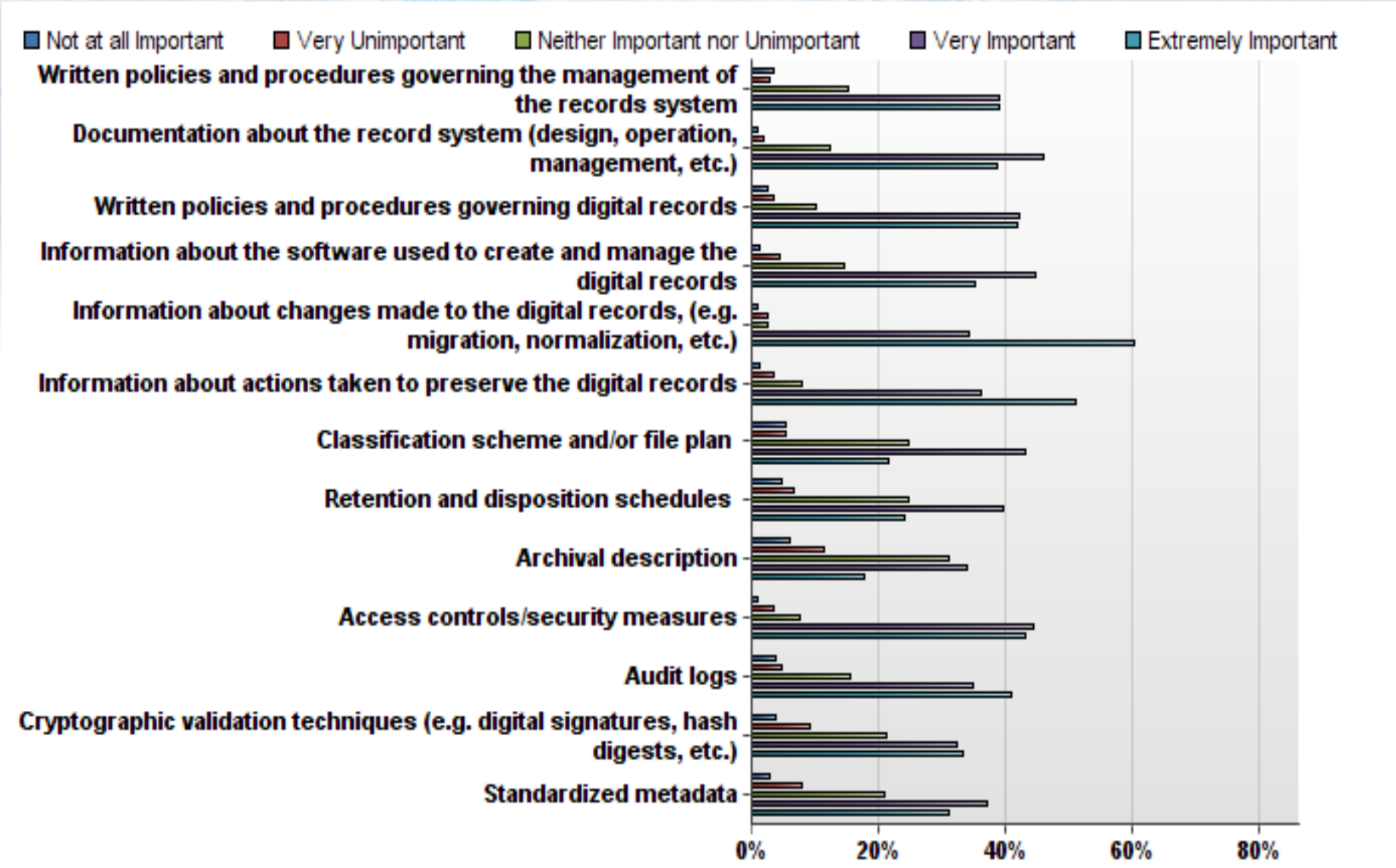
- survey of practitioners
- how their work supports authenticity
- what indicators of authenticity they rely on
- what indicators of authenticity they believe in

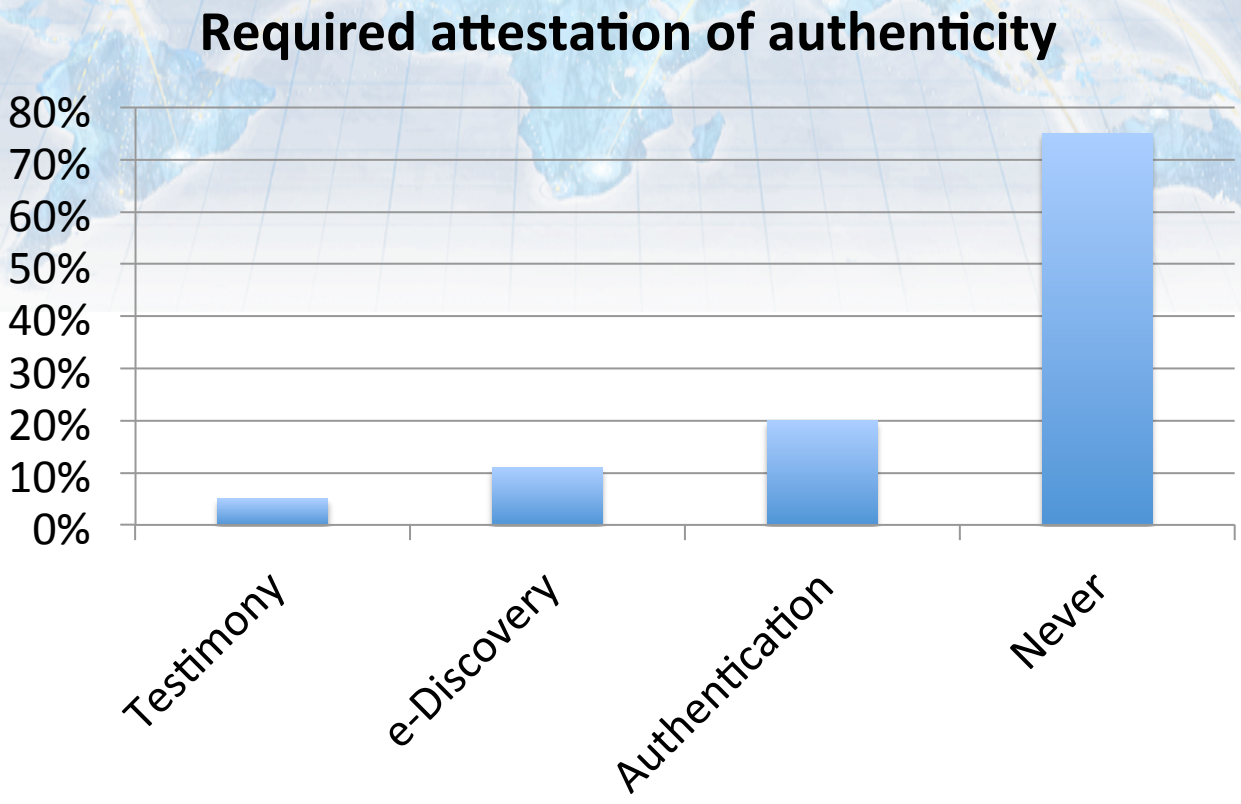
respondents

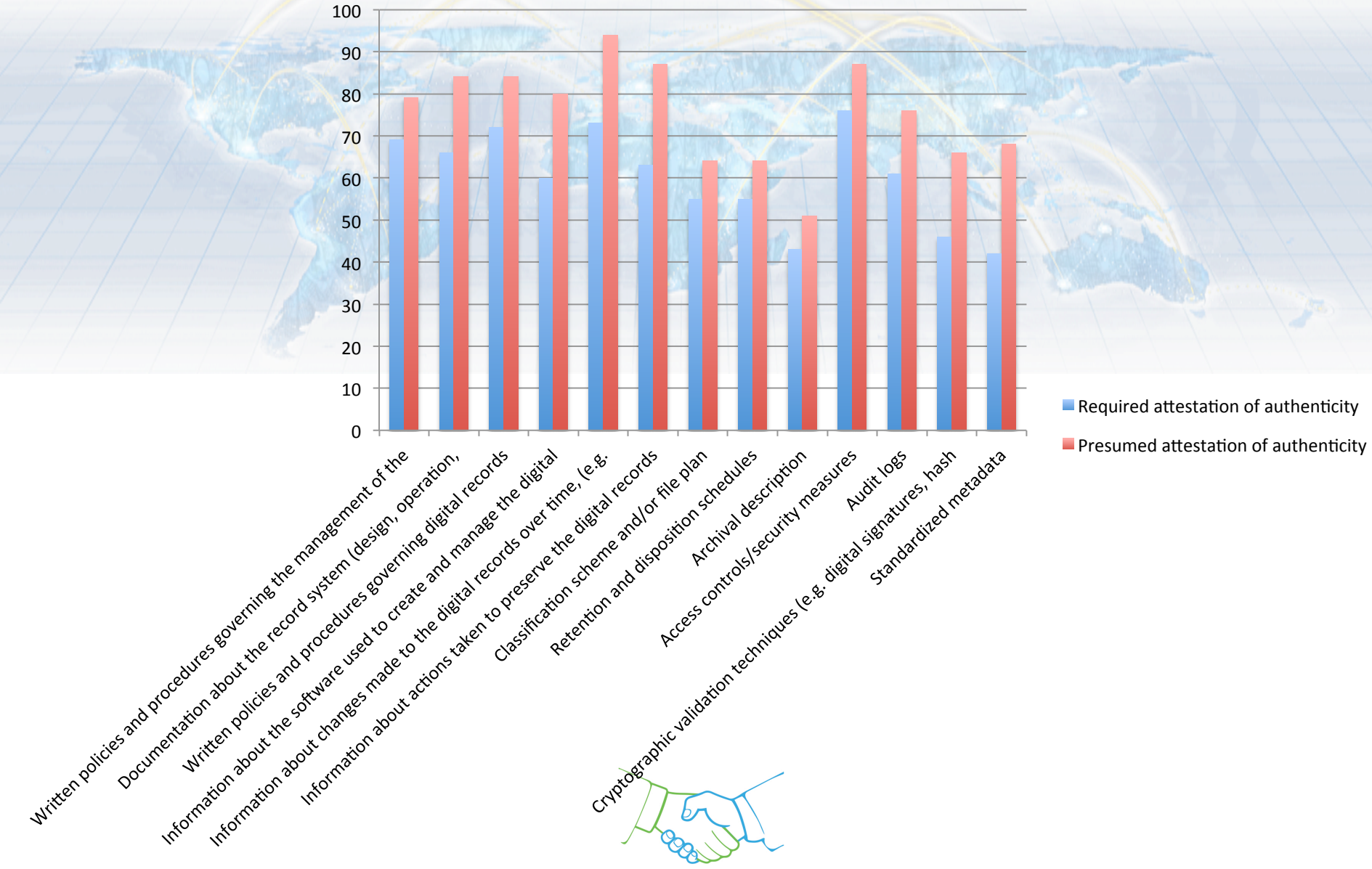


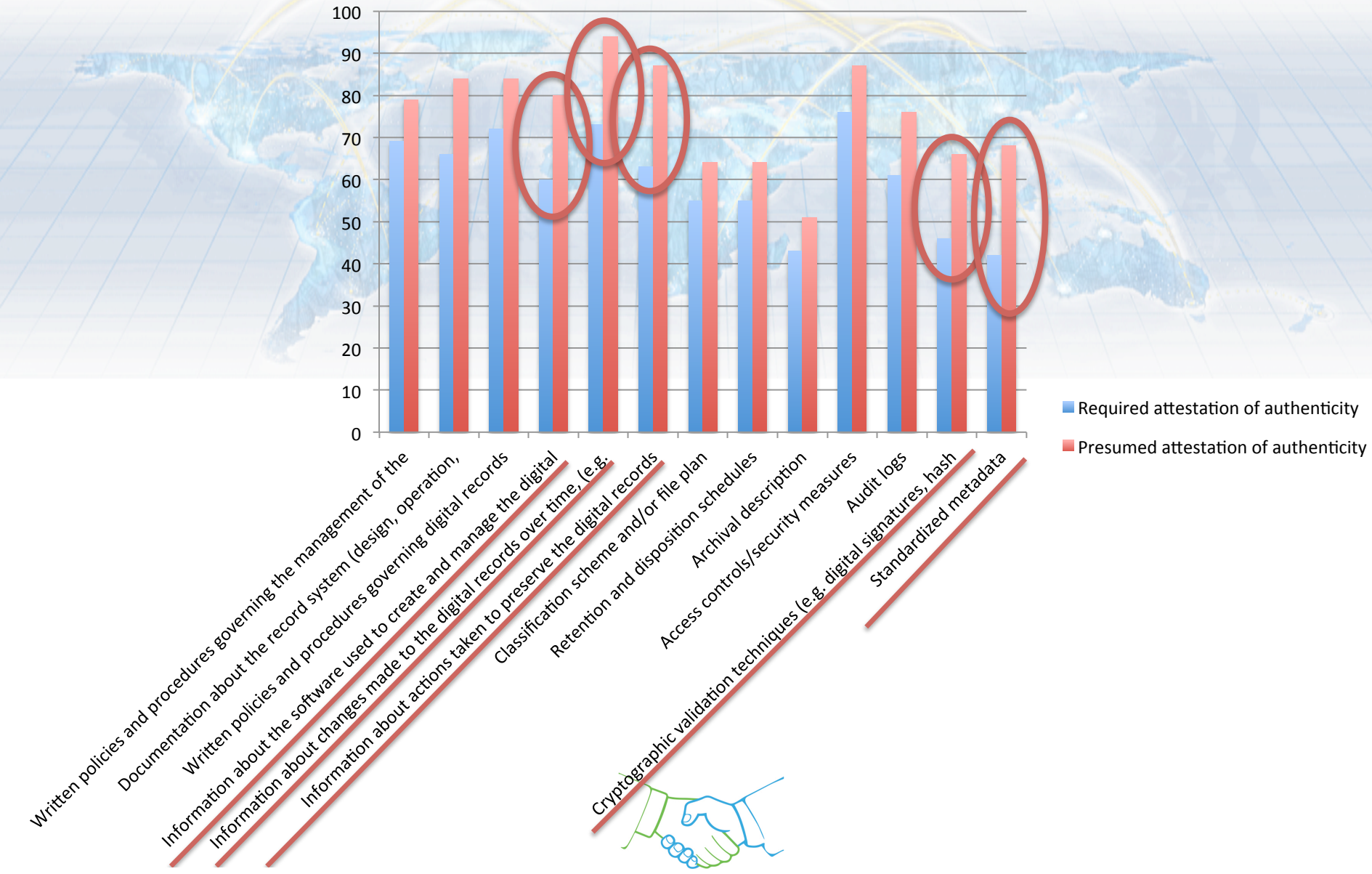

UK
12%
Africa
6%
Asia
2%
Australia/
NZ
8%
South
America
2%
Europe
15%
North
America
55%

frequency of use – social vs technical




Required attestation of authenticity
80%
70%
60%
50%
40%
30%
20%
10%
0%
Testimony
e-Discovery
Authentication
Never


100
90
80
70
60
50
40
30
20
10
0
Written policies and procedures governing the management of the
Documentation about the record system (design, operation,
Written policies and procedures governing digital records
Information about the software used to create and manage the digital
Information about changes made to the digital records over time, (e.g.
Information about actions taken to preserve the digital records
Classification scheme and/or file plan
Retention and disposition schedules
Archival description
Access controls/security measures
Audit logs
Cryptographic validation techniques (e.g. digital signatures, hash
Standardized metadata
Required attestation of authenticity
Presumed attestation of authenticity


100
90
80
70
60
50
40
30
20
10
0
Written policies and procedures governing the management of the
Documentation about the record system (design, operation,
Written policies and procedures governing digital records
Information about the software used to create and manage the digital
Information about changes made to the digital records over time, (e.g.
Information about actions taken to preserve the digital records
Classification scheme and/or file plan
Retention and disposition schedules
Archival description
Access controls/security measures
Audit logs
Cryptographic validation techniques (e.g. digital signatures, hash
Standardized metadata
Required attestation of authenticity
Presumed attestation of authenticity

organizational support

- 54% of respondents reported that their organization's records and information policies did not define or require authenticity of digital material
- 17% did not know if their organization's records and information policies defined authenticity of digital material

practitioners' definitions of authenticity of digital records

- traditional social heuristics preferred in practice
- usual and ordinary course of business
- measures of integrity conflated with authenticity
- bitwise integrity
- pragmatic approach

what essential indicators of authenticity?

- evidence of chain of custody
- controls governing creation & management
- access policies & system security
- => controlling the environment

in depth interviews

Case 1: university archive as a records creator

Case 2: large national memory institution with a robust digital preservation complex

Case 3: open source software product used by the non-for-profit digital preservation sector

conclusion

thank you!

www.interparestrust.org

cmrogers@mail.ubc.ca