"ARCHIVI & COMPUTER" Rivista quadrimestrale

Direttore responsabile Roberto CERRI

Direzione Maria GUERCIO

Comitato scientifico

Francesco CATTANEO, Emilia CENTO, Roberto CERRI, Linda GIUVA, Roberto GRASSI, Marco LATTANZI, Guglielmo LONGOBARDI, Stefano PIGLIAPOCO. Enrico RENDINA, Claudia SALMINI, Maurizio SAVOJA. Luciano SCALA, Gabriella SERRATRICE, Federico VALACCHI, Stefano VITALI, Andrea ZORZI.

Collaboratori internazionali

Francisco BARBEDO, Catherine DHÉRENT, Luciana DURANTI. Ann GILLILAND SWETLAND, Hans HOFMAN, Heather MACNEIL, Seanius ROSS, Ken THIBODEAU.

Segreteria di redazione Prisca GIORDANI, Monica GROSSI, Giovanni MICHETTI, Susanna OREFFICE

Sede della redazione

"ARCHIVI & COMPUTER"

c/o Titivillus Edizioni di Mancini Andrea & C. sas, via Zara n. 58, 56020 Corazzano (PI) Tel. 0571 462825/35 Fax 0571 462700 e-mail: archilab@titivillus.it

Sono disponibili i fascicoli e le annate 1991-2005 (un fascicolo \in 20,00; un'annata \in 50,00; sconto per librerie 20%; sconto per i soci 30%).

Le richieste devono pervenire a **Titivillus Edizioni** di Mancini Andrea & C. sas, via Zara n. 58, 56020 Corazzano (PI) Tel. 0571 462825/35 e-mail: archilab@titivillus.it. I pagamenti possono essere effettuati secondo le seguenti modalità: versamento sul c/c postale n. 25120502 intestato a: Titivillus Edizioni di Mancini Andrea & C sas; bonifico bancario su c/c n, 000010204394 intestato a: Titivillus Edizioni di Mancini Andrea & C. sas, presso Banca di Credito Cooperativo di Cambiano. Agenzia di Corazzano, ABI 08425, CAB 71150, CIN U, IBAN IT 46.

Prezzo

Abbonamento "persona fisica",	€ 32,00
Abbonamento "biblioteche, istituzioni, enti pubblici"	€ 35,00
Annata arrretrata	€ 50,00
Abbonamento estero	€ 60,00
Annata arretrata estero	€ 70,00
Prezzo del singolo fascicolo	€ 13,00
Sconto per librerie	20%
Sconto per soci Archilab	30%

L'abbonamento e la richiesta di numeri arretrati avviene tramite Titivillus Edizioni di Mancini Andrea & C. sas, via Zara n. 58, 56020 Corazzano (PI) Tel. 0571 462825/35 Fax 0571 462700 e-mail: archilab@titivillus.it, I pagamenti possono essere effettuati secondo le seguenti modalità versamento sul c/c postale n. 25120502 intestato a: Titivillus Edizioni di Mancini Andrea & C sas; bonifico bancario su c/c n, 000010204394 intestato a: Titivillus Edizioni di Mancini Andrea & C. sas, presso Banca di Credito Cooperativo di Cambiano, agenzia di Corazzano, ABI 08425, CAB 71150, CIN¹U, IBAN IT 46.

Per i soci Archilab l'abbonamento è già compreso nella quota d'iscrizione annuale.

Autorizzazione del Tribunale di Pisa n. 8 del 23-03-1991. Quadrimestrale - Spedizione in A.P. - 70% - Filiale di Pisa. Proprietà: Archilab, Loggiati di San Domenico, 3 - 56027 San Miniato (PI) Stampa: Tipolitografia Bongi, via A. Conti, 10 - 56027 San Miniato (PI).

I quadrimestre 2006 • Finito di stampare nel mese di ottobre 2006

ISSN 1121-2462

ARCHIVI & COMPUTER AUTOMAZIONE E BENI CULTURALI

Anno XVI

Fascicolo 1/06

Le tecnologie dell'informazione al servizio degli archivi: riflessioni e proposte per la conservazione a lungo termine

INDICE

SAGGI Maria GUERCIO Certezza documentaria e memoria p. 5 digitale: una riflessione sul futuro della funzione archivistica Luciana DURANTI La questione fondamentale: in quali 24 entità digitali si traduce la memoria del futuro? Sauro ORSINI Applicazioni multimediali a costo ri-32 dotto nel lavoro archivistico. Le descrizioni vocali preliminari Seamus ROSS, The role of evidence in establishing 46 Andrew MCHUGH trust in repositories Antonio MASSARI. Gestire la transizione dal sistema 60 Stefano CHIARETTI. cartaceo a quello digitale ottimizzan-Claudio BALBIANI do gli investimenti Francesca MARINI Trusted digital repositories: overview 76 and key issues INTERVENTI Emerging approaches for digital pres-95 ervation in digital libraries: report on the Fifth DELOS International Summer School

Francesca MARINI

Trusted digital repositories: overview and key issues *

Abstract: Questo articolo costituisce un'introduzione al problema dei depositi digitali affidabili, descrivendone alcuni requisiti e problematiche di base, nel contesto di sviluppi teorici e pratici a livello internazionale. Dopo aver dato una definizione di deposito digitale affidabile, l'articolo descrive le strutture coinvolte nella creazione, gestione, mantenimento ed uso dei depositi e poi approfondisce le questioni relative ai diversi tipi di istituzioni, di utenti e di diritti. Successivamente, l'articolo passa ad analizzare alcune questioni chiave, come quelle dei costi e della conservazione, e dà alcuni esempi di lavoro fatto a livello teorico, come lo sviluppo del modello di riferimento OAIS, e di realizzazioni pratiche, come il deposito DSpace del Massachusetts Institute of Technology-MIT. L'articolo si conclude con una breve discussione degli sviluppi futuri e degli interrogativi ancora da risolvere.

1. Introduction

Universities, research centers and other research institutions, memory organizations, such as archives, libraries and museums, as well as private sector organizations, which produce, store, manage and provide access to digital resources need to trust their repositories. A few examples of digital repositories¹ are the California Digital Library (CDL) eScholarship Repository,² the United States National

* This article is based on the briefing paper prepared by the author and discussed with the directors of the ERPANET Project and with Robin Dale, for the ERPANET Workshop "Trusted Repositories for Preserving Cultural Heritage," Rome, 17-19 November 2003.

¹ Examples of digital repositories are also discussed in Abby Smith, *New-model scholarship: how will it survive*? (Council on Library and Information Resources, March 2003) (available at: http://www.clir.org/pubs/reports/pub114/contents.html. Last accessed: 14 December 2004). The ERPANET website has a page, with useful links, dedicated to the topic: "Topic of the Month: Digital Repositories" (available at: http://www.erpanet.org/topic/digitalrepositories/index.php. Last accessed: 14 December 2004).

² Web-site: http://repositories.cdlib.org/escholarship (last accessed: 14 December 2004). The CDL eScholarship Repository is compliant with the Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH) and "offers University of California faculty a central online location for depos-

Archives and Records Administration's Electronic Records Archives (ERA),³ Harward University Library (HUL) Digital Repository Service (DRS),⁴ and the OCLC Digital Archiv⁵. Issues that have been mostly resolved in traditional paper repositories, such as continuing access, security, long-term storage and preservation pose new challenges in the electronic environment. Although many solutions for digital repositories have been found so far, standards and shared ways of addressing problematic issues are not yet widely in place and not all digital repositories may be called "trusted" yet. This is why research groups and organizations (such as the Research Libraries Group-RLG and the Online Computer Library Center-OCLC), universities and other higher education institutions (such as the Massachusetts Institute of Technology-MIT), and research projects, such as InterPARES (International Research on Permanent Authentic Records in Electronic Systems), as well as government research groups, have in recent years started to work on the development of guidelines for the conceptual and practical realization of trusted digital repositories and also on the implementation of actual systems. Some examples will be discussed later in this article. A workshop dedicated to the topic, held in Rome in November 2003, was organized by the ERPANET (Electronic Resource Preservation and Access Network) Project, the Accademia dei Lincei-Centro Linceo Interdisciplinare, and the Fondazione Ezio Franceschini,⁶ and offered an opportunity for discussion and for sharing experiences and expertise.

Focusing only on key issues related to the topic, this introductory article presents an overview of what trusted digital repositories are, with examples of what has been done to date in this area and a specific focus on the work of cultural organizations and institutions that preserve cultural heritage; needs and requirements are

iting working papers, technical reports, research results, datasets with commentary and peer-reviewed series" (from: Open Archives Initiative, *California Digital Library*, in "OAI News", March 2003. Available at: http://www.openarchives.org/news/news2.html#CDL2. Last accessed: 14 December 2004).

³ Web-site: http://www.archives.gov/electronic_records_archives/index.html (last accessed: 14 December 2004).

⁴ Web-site: http://hul.harvard.edu/ois/systems/drs (last accessed: 14 December 2004).

⁵ Web-site: http://www.oclc.org/digitalarchive/default.htm (last accessed: 14 December 2004). See also Pam Kircher, "Nuts and bolts: how do you know what kind you need?" (paper presented at the annual meeting of the Society of American Archivists, Los Angeles, Calif., August 2003); and Dawn Lawson and Phyllis B. Spies, *Developing a trusted digital repository: the OCLC experience*, in "VINE. The Journal of Information and Knowledge Management Systems", 34, no. 1 (2004): 27-32 (available at: http://hermia.emeraldinsight.com/vl=2910937/cl=30/nw=1/rpsv/cw/www/mcb/03055728/v34n1/ contp1-1.htm. Last accessed: 14 December 2004).

The OCLC Digital Archive also uses the work of the OCLC/RLG working group PREMIS (PREservation Metadata: Implementation Strategies) (see PREMIS web-site at: http://www.oclc.org/research/projects/pmwg, Last accessed: 14 December 2004).

⁶ The workshop report, the papers presented and other information are available on the ERPANET web-site at: http://www.erpanet.org/events/2003/rome/index.php. Last Accessed: 14 December 2004.

presented from this point of view. This overview opens with a definition (What is a trusted digital repository?), then briefly discusses the stakeholders involved (Stakeholders). It then addresses the theoretical and practical issues related to the development and implementation of trusted digital repositories, with examples of current research and implementations (What types of institutions have or might have trusted digital repositories?; Who uses trusted digital repositories?; Who has rights and interests in trusted digital repositories?; Some Key theoretical and practical issues in trusted digital repositories; Theoretical development of trusted digital repositories: some examples; Theoretical/practical development of and tools for trusted digital repositories; Implementations of trusted digital repositories: some examples). Finally, it offers some brief remarks about the future and presents some possible questions for further development and discussion (Open questions and next steps in the development of trusted digital repositories).

2. What is a trusted digital repository?

There is not yet a definition commonly agreed upon among different communities; among others, library, archival, museum, and scientific communities may have different needs and therefore have a different view of what a trusted digital repository should be⁷. The work of the library community towards a definition has so far been maybe the most visible, but much is also being done in the archives community⁸. For the scope of this article, the definition offered by the RLG-OCLC Report *Trusted digital repositories: attributes and responsibilities* provides a clear statement and a good starting point for discussion: "A trusted digital repository is one whose mission is to provide reliable, long-term access to managed digital resources to its designated community, now and in the future"⁹. Besides giving this brief definition, the report states that:

⁷ Hans Hofman, electronic mail message to author, 23 October 2003.

⁸ Among the initiatives in the archival community, see the work done by the ISO TC46/SC11 (ISO Technical Committee 46-Information and Documentation/Sub-committee 11-Archives/Records management). See information on the ISO web-site at: http://www.iso.ch/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=4718 (last accessed: 14 December 2004). ISO TC46/SC11 developed the standards ISO 15489-1:2001, Information and documentation – Records management – Part 1: General, ISO/TR 15489-2:2001, Information and documentation – Records management – Part 2: Guidelines, and ISO/TS 23081-1:2004 Information and documentation are an agement processes - Metadata for records – Part 1: Principles. See information at: http://www.iso.ch/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeStandardsListPage. TechnicalCommitteeStandardsListPage.

⁹ RLG (Research Libraries Group)-OCLC (Online Computer Library Center) Working Group on Digital Archive Attributes, *Trusted digital repositories: attributes and responsibilities. An RLG-OCLC Report,* Mountain View, Calif., RLG, May 2002. Available at: http://www.rlg.org/longterm/repositories.pdf. Last accessed: 14 December 2004, p. 5.

"All trusted digital repositories must accept responsibility for the long-term maintenance of digital resources on behalf of its depositors and for the benefit of current and future users; have an organizational system that supports not only long-term viability of the repository, but also the digital information for which it has responsibility; demonstrate fiscal responsibility and sustainability; design its system(s) in accordance with commonly accepted conventions and standards to ensure the ongoing management, access, and security of materials deposited within it; establish methodologies for system evaluation that meet community expectations of trustworthiness; be depended upon to carry out its long-term responsibilities to depositors and users openly and explicitly; have policies, practices, and performance that can be audited and measured; and meet [other] responsibilities"¹⁰ detailed in the report.

Attributes and responsibilities are defined throughout the RLG/OCLC report, which, among other recommendations, proposes that a trusted digital repository be compliant with the OAIS reference model, secure, financially stable, and suitable to user needs. The report discusses policy issues throughout, since policy considerations are a basic component in the development of any trusted digital repository, and in contracting with a third-party provider.¹¹

3. Stakeholders

A digital repository has many different components at its various intellectual and practical levels; therefore many groups of stakeholders are involved. The list below presents some possible categories of stakeholders. These categories are not mutually exclusive and may co-exist within the same institution, for example, in a university that is building a digital repository; in cases like this, the divisions might be more political than functional differences¹². Clusters of roles and responsibilities may be executed or exercised by one group, organization, or individual; there is not a one-to-one relationship between roles and responsibilities and organizations/people¹³.

3.1 The institution or group of institutions establishing and/or participating in the repository.

Some examples: research universities, other cultural institutions, libraries, archives and museums 14

¹⁰ Ibidem.

¹¹ Robin Dale, electronic mail message to author, 13 October 2003.

¹² Ibidem.

¹³ Hans Hofman, electronic mail message to author, 23 October 2003.

¹⁴ For these and other examples, see RLG-OCLC, Trusted digital repositories, pp. 5-7.

3.2 The people who create the content hosted in the repository (content creators). Some examples: scholars, researchers, professionals from different fields, arti-

fact creators and writers. These people may be currently active or may have been active in the past.

3.3 The people who provide the content to the repository (content providers).

Content providers may be the same as the content creators: for example, a professor might write a paper and make it available directly through a university digital repository. In another instance, content providers may be the people who receive and manage the content once created: for example, a scholar might write an article and have it published in an online journal; in this case, it is the journal that will act as a provider and make the article available to the repository.

3.4 The people who adapt the content to the digital environment.

Some materials stored in a digital repository may exist in non-digital form outside the repository, as in the case of text, photographs or artifacts that have been digitized. Other materials may be born digital, but be in a format that is not compatible with the repository's capability or preferred formats: in this case the original digital object needs to be transferred and adapted to the new environment¹⁵. People with specific technical expertise within (and sometimes outside) the organization may be in charge of implementing the necessary transformations.

3.5 The people who develop the technology and tools used in the repository.

For example, private companies, hardware and software developers. Repositories usually acquire and use technology and tools developed by outside providers; sometimes, though, they internally develop software or more closely collaborate with technology providers. A recent collaboration is the one between the Hewlett-Packard Company and the Massachusetts Institute of Technology (MIT), which together developed DSpace, an open-source, long-term digital storage repository system for MIT¹⁶.

3.6 The people who design and manage the system and provide access to the repository's content at the technical level.

For example, system designers, system administrators and information technology experts. This group may comprise internal personnel of one or more institutions involved in the repository and/or third-party contractors and service providers. 3.7 The people who manage the system and provide access to the repository's content at the intellectual level.

For example, archivists and librarians. This group of stakeholders might (and should) also be involved in the system design.

3.8 The people who manage the system and provide access to the repository's content at the administrative level.

For example, archives or library directors and institutional administrative personnel. Another instance might be the joint responsibility shared in the relationship between a third-party provider and a contracting institution¹⁷.

3.9 The people who use the content stored in the repository.

This group may comprise internal users, such as students and professors at a parent institution, or external users, for example, users from other institutions and the general public. Types of users and user needs may change and evolve over time¹⁸.

3.10 The people who hold rights to the content of the repository and/or to the technology necessary to access and use the content.

Due to the complexity of digital repositories, there may be a large number of people or groups of people holding rights. Perhaps with the exception of the groups listed under 3.4, 3.8, and 3.9 (in part), almost all other stakeholders discussed above might have rights to either the repository's content and/or its technology and design. For example: an institution might have rights to the content of its repository; a journal might have rights to an article stored in the repository; a software company might have rights to a specific software program necessary to access the repository's content. It is important to remember that custody does not always imply ownership¹⁹. This archival principle remains particularly relevant in the electronic environment. In fact, implementing all the necessary levels of control to content access and use is a fundamental aspect of managing digital repositories²⁰.

Lib Magazine", 9 (January 2003) (available at: http://www.dlib.org/dlib/january03/smith/01smith. html. Last accessed: 14 December 2004).

¹⁷ Robin Dale, electronic mail message to author, 13 October 2003.

¹⁸ See, for example, the discussion of users' needs in RLG-OCLC, *Trusted digital repositories*, pp. 27 and throughout the document.

¹⁹ "Custody does not always include legal ownership, or the right to control access to records": from the entry "Custody," in Lewis J. Bellardo and Lynn Lady Bellardo, *A glossary for archivists, manuscript curators and records managers*, Chicago, The Society of American Archivists, 1992, p. 9.

²⁰ See, for example, RLG-OCLC. Trusted digital repositories, pp. 18-19.

¹⁵ See, for example, *ibidem*, pp. 21-23.

¹⁶ See, for example, *The DSpace Project*, in "MIT Faculty Newsletter", 12 (April-May 2000) (available at: http://dspace.org/news/articles/dspace-project.html. Last accessed: 14 December 2004) and MacKenzie Smith, Mick Bass, Greg McClellan, Robert Tansley, Mary Barton, Margret Branschofsky, Dave Stuve, and Julie Harford Walker, *DSpace: An Open Source Dynamic Digital Repository*, in "D-

3.11 Government agencies and other political or policy bodies at the international, national and local level that may devise and implement legislation, rules and policies that affect digital repositories.

The stakeholders in this group might be, for example, governments, state and local administrations. Applicable laws, rules, regulations and policies at the national and local level will affect how the repository and its content are managed and made accessible to users. If a repository implies cooperation among different countries, international rules may also apply. Complications in the management of digital repositories might arise from the potential high number of stakeholders in this group and from potentially conflicting rules and policies.

Every group listed above would deserve a separate, detailed analysis, along with a discussion of the specific implications of its role in trusted digital repositories. Some issues are discussed in more detail below.

4. What types of institutions have or might have trusted digital repositories?

Institutions interested in establishing trusted digital repositories may already have a collection of digital materials or may want to start one. The RLG-OCLC report on *Trusted Digital Repositories* presents five scenarios that discuss examples of institutions with specific needs and requests²¹. The scenarios include cultural and research institutions and organizations: a national library, a large university library, a museum, a virtual digital repository for e-journals shared by different institutions, and a small cultural institution²². These are just a few examples, to which we can add more, such as other types of libraries, archives, research centres and institutes, and historical societies²³. The needs of each institution or organization vary, because their missions, their activities, their holdings and their users vary. These needs have to be taken into account when developing trusted digital repositories.

5. Who uses trusted digital repositories?

User communities and needs vary from repository to repository and evolve over time. A few examples: A university's collection mostly serves the research and study activities of faculty and students; access to collections or specific documents may sometimes be restricted and the documents stored could be anything, from

²³ These examples are based on the list of participating institutions in Appendix B of Margaret Hedstrom and Sheon Montgomery, *Digital preservation needs and requirements in RLG member institutions*. A study commissioned by the Research Libraries Group. Mountain View, Calif., RLG, December 1998, (available at: http://www.rlg.org/legacy/preserv/digpres.html; HTML final version, 22 January 1999. Last accessed: 14 December 2004. Also available in PDF format: http://www.rlg. org/legacy/preserv/digpres.pdf. Last accessed: 14 December 2004).

datasets to research papers, stemming from a variety of disciplines and activities. The collection of a public library is usually accessible to the general public and geared to more general topics and interests. The collections of a national library or national archives may present access restrictions and also cover scholarly topics, serving a range of users from non-expert to highly specialized ones. An e-journals repository may be geared to specific communities or may be available to a more general public and may or may not present access restrictions and use restrictions. Museum collections online are usually accessible to the general public, but with restrictions as far as downloading and using images.

Users of trusted digital repositories might be internal or external to the institutions involved with the repositories. Both internal and external users may belong to different communities of practice or interest; for example, the users of a university repository may be part of different departments and prefer different ways of submitting, accessing and using the stored information²⁴.

Once a trusted digital repository is established, its usability should be periodically tested, to make sure that users can find and access what they need in the most uncomplicated way possible²⁵.

6. Who has rights and interests in trusted digital repositories?

As noted earlier, many stakeholders have rights and interests in trusted digital repositories. In the establishment and management of repositories, rights assessment and clearance is a major concern, and may lead to access and use restrictions. All rights holders have to be identified and their requests have to be met or negotiated when appropriate. Copyright legislation has to be constantly monitored, both at the national and also international level, depending on the repository's level of accessibility; what is legal in one country may not be legal in another. Institutions involved with digital repositories might also sometimes need to make their voice heard in the copyright legislative arena.

7. Some key theoretical and practical issues in trusted digital repositories

The literature cited throughout this article, especially the RLG/OCLC report and the OAIS document²⁶, addresses the theoretical and practical issues presented

²⁴ See, for example, the discussion of "communities" in Smith et al., *DSpace*, p. 2. Although it covers more general concepts and it is not specifically geared towards the electronic environment, it is also important to mention here Etienne Wenger's work on "communities of practice": see Etienne Wenger, *Communities of practice: learning, meaning and identity*, Cambridge, United Kingdom, Cambridge University Press, 1998. Reprint, 1999.

²⁵ On usability testing, see, for example, Rosalie Lack, *An introduction to usability testing* (paper presented at the annual meeting of the Society of American Archivists, Los Angeles, Calif., August 2003).

²⁶ Consultative Committee for Space Data Systems, *Reference Model for an Open Archival Information System (OAIS)/CCSDS 650.0-B-1.* Blue Book 1 (January 2002) (available at: http://ssdoo.gsfc.nasa.gov/nost/wwwclassic/documents/pdf/CCSDS-650.0-B-1.pdf. Last accessed: 14 December 2004).

²¹ RLG-OCLC, *Trusted digital repositories*, pp. 5-7.

²² Ibidem.

by trusted digital repositories in great detail. This section therefore presents only a few considerations and identifies possible key elements and issues, without thoroughly discussing and analyzing them and their implications²⁷.

7.1 Cost²⁸

Cost has to be factored in any decisions taken at the design, implementation and everyday use levels. Funds have to be secured on a constant basis, because a sudden lack of funding could terminate the existence of some digital objects in the system and cripple important system functions.

7.2 Digital resources

Digital resources are complex objects that require intensive action in order to be preserved and made available over time. Although access restrictions have to be implemented when necessary, stored materials have to be made accessible to users in the simplest way possible. The RLG/OCLC report also points out that the OAIS reference model calls for the information to be independently understandable to the user community²⁹ and discusses how the digital object has to go through many levels before becoming humanly understandable³⁰. It is also important to remember that it is not always straightforward to agree on the precise definition of what is a digital object in a system³¹.

7.3 Flexibility of the system

Flexibility is essential in the design and implementation of trusted digital repositories. Repositories have to be able to accommodate the changing needs of institutions and users and also the new digital formats that may appear in the future. The system has also to be flexible because a repository may contain several digital archives³².

²⁷ For discussion related to these issues, see also ERPANET, *ErpaWorkshop: Trusted Repositories* for Preserving Cultural Heritage. Final Report (available at: http://www.erpanet.org/events/2003/ rome/Rome-report%20translation_final.pdf. Last accessed: 14 December 2004), and the workshop's presentation by Robert Kahn, "Reflections on the digital object architecture" (available at: http://www. erpanet.org/events/2003/rome/presentations/presentation_Kahn.pdf. Last accessed: 14 December 2004).

²⁸ As part of its "erpaGuidance" activities (see: http://www.erpanet.org/guidance/index.php; last accessed 14 December 2004). ERPANET has developed a *Cost orientation tool* (September 2003) (available at: http://www.erpanet.org/guidance/docs/ERPANETCostingTool.pdf. Last accessed: 14 December 2004).

²⁹ See RLG-OCLC, *Trusted digital repositories*, pp. 27-28. See also Consultative Committee for Space Data Systems, *Reference Model for an Open Archival Information System*: 1-10 (entry "Independently Understandable").

³⁰ RLG-OCLC, Trusted digital repositories, pp. 27-28.

³¹ See, for example, Nancy Y. McGovern, *Mapping organizational activities to the OAIS Reference Model*, paper presented at the annual meeting of the Society of American Archivists, Los Angeles, Calif., August 2003.

³² *Ibidem.* Cornell's Common Depository System, presented later in this paper, is a good example of flexibility, since it is open to having different systems meet different needs.

7.4 Interoperability

A major responsibility of the repository is compatibility and interoperability with other systems so that a broad variety of access interfaces can be applied, used and developed without being affected by the constraints of the archive architecture. Repositories should be able to talk to each other, especially when shared responsibility and interoperability agreements are in place.

7.5 Long-term access

Long-term access implies preservation, with attention to the digital preservation strategies currently available, as well as new emerging ones. One of the main goals of trusted digital repositories is to preserve over time the electronic materials stored in them. Preservation has to be addressed from the system's design stage and then constantly maintained. There exist different levels of access and services,³³ which might also have an impact on the trustworthiness of the repository. Many issues should be further investigated, like the one that in a trusted digital repository the "archive" should actually be separate from the delivery system³⁴.

7.6 Metadata

All the metadata necessary for the identification, description, management, retrieval and distribution of digital objects have to be used.³⁵ Metadata will also have an impact on cost³⁶.

³³ See William G. LeFurgy, *Levels of service for digital repositories*, in "D-Lib Magazine" 8 (May 2002) (available at: http://www.dlib.org/dlib/may02/lefurgy/05lefurgy.html. Last accessed: 14 December 2003).

³⁴ Robin Dale, electronic mail message to author, 13 October 2003, and Paul Conway, *Digital technologies and preservation*, paper presented at the annual meeting of the Society of American Archivists, Birmingham, Ala., August 2002 (available at: http://www.lib.duke.edu/its/director/presentations/SAA-Birmingham.pdf. Last accessed: 14 December 2004). The approach of separating archiving from access was taken, for example, in the development of the Florida Center for Library Automation (FCLA) digital archive: see Priscilla Caplan, *Building a digital preservation archive: tales from the front*, in "VINE. The Journal of Information and Knowledge Management Systems" 34, no.1 (2004): 38-42; in particular page 39 (available at: http://hermia.emeraldinsight.com/vl=2910937/cl=30/nw=1/rpsv/cw/ www/mcb/03055728/v34n1/contp1-1.htm. Last accessed: 14 December 2004).

³⁵ A number of international groups are addressing metadata. Relevant information may be found in the papers presented at the ERPANET Training Seminar on "Metadata in Digital Preservation," 3-5 September 2003, Marburg, Germany, available at: http://www.erpanet.org/www/products/marburg/marburg.htm (last accessed: 14 December 2004). See also: OCLC/RLG PREMIS (PREservation Metadata Implementation Strategies) Working Group, *Implementing preservation repositories for digital materials: current practice and emerging trends in the cultural heritage community*. A Report by the PREMIS Working Group (Dublin, OH., and Mountain View, Ca, OCLC-Online Computer Library Center and RLG-Research Libraries Group, September 2004), (available at: http://www.oclc.org/research/projects/pmwg/surveyreport.pdf. Last accessed: 14 December 2004).

³⁶ Robin Dale, electronic mail message to author, 13 October 2003.

7.8 Reliability

Reliability is a key concern in the management of digital materials; this concept is often associated with the one of authenticity and also of trustworthiness. These concepts, which were central to the research of the InterPARES 1 project, are interpreted differently in different contexts³⁷. These different interpretations are key for defining a digital repository, since what different contexts need influences the concept of digital repository; for example, archives have other needs than libraries³⁸.

7.9 Unique identifiers³⁹

Especially when repositories are shared among several institutions, digital materials need to be identified in a unique manner, so to avoid confusion in use and retrieval. There is discussion on whether identifiers should be globally unique or locally unique⁴⁰.

Many other elements not presented here also enter in the design and management of trusted digital repositories⁴¹.

8. Theoretical development of trusted digital repositories: some examples 8.1 Reference Model for an Open Archival Information System (OAIS Reference Model)

The Reference Model for an Open Archival Information System (OAIS reference model)⁴² represents the starting point for much research and many implemen-

³⁷ See the InterPARES 1 report: InterPARES Project, *The long-term preservation of authentic electronic records: findings of the InterPARES Project*, Vancouver, BC, Canada: InterPARES Project. September 2002, (available at: http://www.interpares.org/book/index.htm, Last accessed: 14 December 2004). See also one of the reports of the InterPARES Authenticity Task Force: Ciaran Trace, *Applying content analysis to case study data: a preliminary report*, Los Angeles, Calif., University of California, Los Angeles-Department of Information Studies, 12 June 2001 (available at: http://www.interpares.org/documents/interpares_ApplyingContentAnalysis.pdf. Last accessed: 14 December 2004). The RLG/OCLC Report also has an appendix on the evolution of the concept of trust: RLG-OCLC, *Trusted digital repositories*, Appendix B: "The Evolution of 'Trust' in Computing Systems", pp. 49-54.

³⁸ Hans Hofman, electronic mail message to author, 23 October 2003.

³⁹ An ERPANET Seminar on "Persistent Identifiers" was held in Cork on 17-18 June 2004. See the web-site at: http://www.erpanet.org/events/2004/cork/index.php. Last accessed: 14 December 2004.

⁴⁰ Robin Dale, electronic mail message to author, 13 October 2003.

⁴¹ Administrative responsibility, organizational reliability, financial sustainability, technological and procedural suitability, system security and procedural accountability are also critical issues in this area and would require further discussion (Robin Dale, electronic mail message to author, 13 October 2003). See also Seamus Ross, *National Library of New Zealand: digital library development review. Final report.* Wellington, New Zealand, National Library of New Zealand, July 2003 (available at: http://www.natlib.govt.nz/files/ross_report.pdf. Last accessed: 14 December 2004).

⁴² See Consultative Committee for Space Data Systems. Reference Model for an Open Archival Information System (OAIS). tations. Developed by the Consultative Committee for Space Data Systems Panet 2⁴³, the OAIS model has been used as a framework in research projects, such as the InterPARES Project⁴⁴ and in the design and realization of digital archives⁴⁵ and university digital libraries. In the development of university digital libraries, the OAIS model has often been used along with the RLG/OCLC recommendations (which were also developed from the OAIS model) on attributes and responsibilities of trusted digital repositories.⁴⁶

The OAIS model does not need to be presented here in detail.⁴⁷ It is now a published international standard (ISO 14721: 2003 Reference Model for an Open Archival Information System-OAIS).⁴⁸ Its development started in 1995⁴⁹ and the document describing its final version was published in 2002⁵⁰. Presented by the Consultative Committee for Space Data Systems (CCSDS) "for use in developing a broader consensus on what is required for an archive to provide permanent, or indefinite long-term, preservation of digital information"⁵¹, this document "establishes a common framework of terms and concepts which comprise an Open Archival Information System (OAIS)"⁵². The document has used previous work by RLG and the Commission on Preservation and Access⁵³ as "the basis for the Preserva-

⁴³ See, for example, John Garrett, *US efforts towards ISO archiving standards. Overview* (available at: http://ssdoo.gsfc.nasa.gov/nost/isoas/us/overview.html. Last revised: 24 September 2004. Last accessed: 14 Dacember 2004).

⁴⁴ See, for example, InterPARES Project, *The Long-term Preservation of Authentic Electronic Records*. The InterPARES Project is currently in its second phase of research.

⁴⁵ Among other digital archives initiatives, see the United States National Archives and Records Administration's Electronic Records Archives (ERA) (http://archives.gov/electronic_records_archives/about_era.html. Last accessed: 14 December 2004) and the OCLC Digital Archive (http:// www.oclc.org/digitalarchive/default.htm. Last accessed: 14 December 2003). On the OCLC Digital Archive implementation of OAIS, see also Kircher, "Nuts and Bolts."

⁴⁶ See, for example, McGovern, Mapping organizational activities.

⁴⁷ Information about the OAIS Reference Model may also be found in the papers presented at the ERPANET OAIS Training Seminar, København, 28-29 November 2002 (available at: http://www.erpanet.org/www/products/copenhagen/copenhagen.htm; last accessed: 14 December 2004).

⁴⁸ See the "ISO 14721:2003

Space data and information transfer systems -- Open archival information system -- Reference model" on the International Organization for Standardization (ISO) web-site at: http://www.iso.ch/iso/en/ CatalogueDetailPage.CatalogueDetail?CSNUMBER=24683 (last accessed: 14 December 2004).

⁴⁹ See John Garrett and Donald Sawyer, *Archive reference model gains wide acceptance*, September 2000 (available at: http://nssdc.gsfc.nasa.gov/nssdc_news/sept00/archive_ref_model.html. Last accessed: 14 December 2004).

⁵⁰ Consultative Committee for Space Data Systems, *Reference Model for an Open Archival Information System*.

⁵¹ Ibidem, p. iii.

⁵² Ibidem.

⁵³ John Garrett and Donald Waters, *Preserving digital information: report of the Task Force on Archiving of Digital Information*, Washington, DC, Commission on Preservation and Access, and Mountain View, Calif., RLG, May 1996 (available at: http://www.rlg.org/ArchTF/index.html. Last accessed: 14 December 2004). tion Description Information in the OAIS Information Model"⁵⁴, part of the OAIS reference model. As noted in the InterPARES 1 Project's Preservation Task Force report, "the [OAIS] reference model is intended to apply to any type of information, not just records. For example, the information preserved in an OAIS might be scientific data, or it might be information about physical objects in a museum"⁵⁵.

8.2 RLG-OCLC Report on attributes and responsibilities of trusted digital repositories

Building on the OAIS model, RLG and OCLC developed a document on the attributes and responsibilities of trusted digital repositories, released in its final version in 2002⁵⁶ (a draft report was released in August 2001). The work that led to the final report started in March 2000, when, targeting "large-scale, heterogeneous collections held by cultural organizations"⁵⁷, "RLG and OCLC began a collaboration to establish attributes of a digital repository for research organizations, building on and incorporating the emerging international standard of the Reference Model for an Open Archival Information System (OAIS)"⁵⁸. The RLG/OCLC report is discussed throughout this article.

8.3 The InterPARES 1 Project

The InterPARES 1 Project (1999-2001)⁵⁹, which aimed at developing "the theoretical and methodological knowledge required for the long-term preservation of the authenticity of records created in electronic systems"⁶⁰, has used the OAIS reference model mostly in the development of its preservation function model⁶¹, The project has conducted a series of case studies in different countries and contexts, and identified how existing systems ensure the authenticity of the records that they hold. Benchmark and baseline requirements supporting this purpose have emerged from case study analysis and from the theoretical foundations of the project⁶². Through the work of its four task forces – Authenticity, Appraisal, Preserva-

⁵⁴ Consultative Committee for Space Data Systems, *Reference Model for an Open Archival Information System*: B-1. See also: 4-27 to 4-29.

⁵⁵ InterPARES Project. The Long-term Preservation of Authentic Electronic Records-Preservation Task Force Report: 9.

⁵⁶ RLG-OCLC, Trusted Digital Repositories.

57 Ibidem, p. 1.

58 Ibidem.

⁵⁹ See the project's web-site, available at: http://www.interpares.org/index.htm (last accessed: 14 December 2004).

60 Ibidem.,"The InterPARES 1 Project".

⁶¹ See InterPARES Project, Preservation Task Force Report, especially pages 9 and 10.

⁶² InterPARES Project-Authenticity Task Force, *Requirements for Assessing and Maintaining the Authenticity of Electronic Records* (March 2002) (available at: http://www.interpares.org/display_file. cfm?doc=ip1_authenticity_requirements.pdf. Last accessed: 14 December 2004).

tion, and Strategy – the project has developed a solid knowledge base, recommendations, and models, which provide essential guidance in the design and realization of trusted repositories⁶³.

9. Theoretical/practical development of and tools for trusted digital repositories: some examples

9.1 The Cedars Project and the Cedars Distributed Digital Archiving Prototype System

The Cedars (Curl Exemplars in Digital Archives) Project "began in April 1998 and ended in March 2002. Its broad objective was to explore digital preservation issues"⁶⁴. The Cedars Distributed Digital Archiving Prototype System, based on the OAIS reference model, was developed by the project⁶⁵, which "built this system in order to test its methodologies; and primarily to prove that digital preservation was a soluble problem, since this system demonstrated how it could be solved"⁶⁶.

9.2 The Fedora Project

"In September 2001, the University of Virginia was awarded a grant from the Andrew W. Mellon Foundation to develop the first digital object repository management system based on the Flexible Extensible Digital Object and Repository Architecture (Fedora). The Digital Library Research Group at Cornell University originally developed Fedora under a National Science Foundation Grant. Fedora is one of a number of repository architectures that have been proposed over recent years for use in digital libraries"⁶⁷. The project has developed a "new system, designed to be a foundation upon which interoperable web-based digital libraries, institutional repositories and other information management systems can be built, [which] demonstrates how distributed digital library architecture can be deployed using web-based technologies, including XML and Web services"⁶⁸.

⁶³ See InterPARES Project, *The Long-term Preservation of Authentic Electronic Records-Preservation*, as well as the other documents and information available on the web-site.

⁶⁴ Cedars Project web-site, available at: http://www.leeds.ac.uk/cedars (last accessed: 14 December 2004).

⁶⁵ See Kelly Russell and Derek Sergeant, *The Cedars Project: implementing a model for distributed digital archives*, in "RLG DigiNews", 3 (June 15, 1999) (available at: www.rlg.org/legacy/preserv/diginews/diginews3-3.html. Last accessed: 14 December 2004), and The Cedars Project, *Cedars Guide to the distributed digital archiving prototype* (Cedars Project, March 2002) (available at: http://www. leeds.ac.uk/cedars/guideto/cdap. Last accessed: 14 December 2004).

66 Cedars Project, Cedars Guide, pp. 3.

⁶⁷ Thornton Staples, Ross Wayland, and Sandra Payette, *The Fedora project: an open-source digital object repository management system*, in "D-Lib Magazine", 9 (April 2003) (available at: http://www. dlib.org/dlib/april03/staples/04staples.html. Last accessed: 14 December 2004).

⁶⁸ Project web-site: http://www.fedora.info/index.shtml (last accessed: 2 November 2003). Fedora 1.2.1 may be downloaded from this web-site.

9.3 LOCKSS

Stanford University is developing the LOCKSS (Lots of Copies Keep Stuff Safe)⁶⁹ system and program, with financial support from the Andrew W. Mellon Foundation. The LOCKSS Program builds tools and provides support to libraries and publishers⁷⁰. The LOCKSS software has been under development since 1999 and is distributed as open source⁷¹. It "provides librarians with an easy and inexpensive way to collect, store, preserve, and provide access to their own, local copy of authorized content they purchase. Running on standard desktop hardware and requiring almost no technical administration, LOCKSS converts a personal computer into a digital preservation appliance, creating low-cost, persistent, accessible copies of e-journal content as it is published"⁷². LOCKSS promotes and enables publishers' understanding of the importance of archiving and long-term preservation⁷³ and helps them provide content to libraries and ensure perpetual access⁷⁴.

10. Implementations of trusted digital repositories: some examples

10.2 Cornell University Library Common Depository System (CDS)

Cornell University Library and Cornell Information Technologies (CIT) have developed a digital repository using both the RLG/OCLC work on Trusted Digital Repositories and the OAIS reference model, and integrating them with additional research tailored to their own needs⁷⁵. The Common Depository System (CDS) initiative began in March 2001⁷⁶. Cornell University has also joined the DSpace Federation⁷⁷. Cornell's approach shows openness to having different systems meet different needs and is a good example of flexibility.

10.3 DSpace

The Massachusetts Institute of Technology (MIT) started collaboration with Hewlett-Packard Company (HP) in March 2000 to build a digital repository that could accommodate MIT's and other research institutions' and organizations' needs

⁶⁹ LOCKSS was presented in session five of the ERPANET workshop on trusted digital repositories.

⁷⁰ LOCKSS web-site ("Permanent Publishing on the Web") (available at: http://lockss.stanford.edu. Last accessed 14 December 2004). On LOCKSS see Michael A. Keller, Victoria A. Reich, and Andrew C. Herkovic, *What is a library anymore, anyway*?, in "First Monday", 8 (May 2003) (available at: http://www.firstmonday.org/issues/issue8_5/keller/index.html. Last accessed 14 December 2004).

⁷¹ LOCKSS web-site, http://lockss.stanford.edu/about/about.htm (last accessed: 14 December 2004).
⁷² Ibidem.

⁷³ LOCKSS web-site, http://lockss.stanford.edu/publishers/publishers.htm (last accessed: 14 December 2004).

⁷⁴ LOCKSS web-site, http://lockss.stanford.edu/about/about/about.htm (last accessed: 14 December 2004).
 ⁷⁵See Nancy Y. McGovern, *Mapping organizational activities*, pp. 4 (handout).

⁷⁶ See "Common Depository System (CDS)" on Cornell University Library's web-site (available at: http://www.library.cornell.edu/iris/dpo/cds.html. Last accessed: 14 December 2004).

⁷ See Nancy Y. McGovern, *Mapping organizational activities*, pp. 4 (handout).

to store, manage and access their "intellectual output in digital formats"⁷⁸. The digital repository, DSpace, became a new service of the MIT libraries in October 2002 and was then released as a system worldwide in November 2002⁷⁹. Institutions other than MIT may freely adopt DSpace as an open source system, under the terms of the Berkeley Standard Distribution License (BSD), an open source license⁸⁰. Institutions may run the system as-is or modify it according to their needs; HP and MIT support a federation of the system's adopters (DSpace Federation)⁸¹.

DSpace allows "collecting, managing, indexing, and distributing digital items"⁸². DSpace use of metadata is partially based on the OAIS framework⁸³. DSpace implements the Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH)⁸⁴; its metadata is based on Dublin Core and DSpace is also working with the METS (Metadata Encoding and Transmission Standard) community⁸⁵.

10.4 Koninklijke Bibliotheek (KB, the National Library of the Netherlands)

The Koninklijke Bibliotheek (KB, the National Library of the Netherlands)⁸⁶ was, along with the Cedars project in the UK, one of the first groups involved in implementing an OAIS-based repository. Its e-Depot (DNEP-Depot van Nederlandse Elektronische Publicaties)⁸⁷, which stores all kinds of electronic publications (off-line and on-line) is also based on the recommendations of the European project

⁷⁸ Smith et al., DSpace, p. 1.

⁸⁰ *Ibidem.* For the Berkeley Standard Distribution License (BSD), see the Open Source Initiative (OSI) web-site at: http://www.opensource.org/licenses/bsd-license.php (last accessed: 14 December 2004). More information on DSpace can be found at www.dspace.org (last accessed, 14 December 2004); the actual system is available for download from: http://sourceforge.net/projects/dspace (last accessed: 14 December 2003). A "DSpace Installation Training Workshop" was jointly organized by ERPANET, the Cambridge-MIT Institute (CMI) and DSpace@Cambridge at Glasgow University, 9-11 September 2003 (see the web-site at: http://www.erpanet.org/events/2003/glasgow/index.php. Last accessed: 14 December 2004). DSpace was also discussed in session five of the ERPANET workshop on trusted digital repositories.

81 Smith et al., DSpace, pp. 1 and 7.

83 Ibidem, pp.2.

⁸⁴ Ibidem, pp. 4. On the Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH), see the Open Archives Initiative web-site at: http://www.openarchives.org (last accessed: 14 December 2004).

⁸⁵ Smith et al., *DSpace*, pp. 2. About the Metadata Encoding and Transmission Standard (METS), see the Library of Congress web-site at: http://www.loc.gov/standards/mets (last accessed: 14 December 2004).

⁸⁶ The Koninklijke Bibliotheek (KB) web-site is available at: www.kb.nl (last accessed: 14 December 2004).

⁸⁷ On KB e-Depot see the web-site in English at http://www.kb.nl/dnp/dnep-en.html (last accessed: 14 December 2004). See also Erik Oltmans and Hilde van Wijngaarden, *Digital preservation in practice: the e-depot at the Koninklijke Bibliotheek*, in "VINE: The Journal of Information and Knowledge Management Systems", 34, no. 1 (2004): 21-26 (available at: http://hermia.emeraldinsight. com/vl=2910937/cl=30/nw=1/rpsv/cw/www/mcb/03055728/v34n1/contp1-1.htm. Last accessed: 14 December 2004).

⁷⁹ Ibidem.

⁸² Ibidem, pp. 5.

NEDLIB (Networked European Deposit Library)⁸⁸. KB developed its deposit system for electronic publications in collaboration with IBM The Netherlands, which in 2002⁸⁹ delivered the Digital Information Archiving System (DIAS)⁹⁰. According to experts in the field, the KB system is one of the closest to trusted digital repository status; it addresses the preservation planning aspects of an OAIS system, and the signed agreements with major publishers provide long-term access⁹¹.

In the Netherlands, there are also other initiatives currently being implemented, such as the SURF Foundation program Digital Academic Repositories (DARE), "a joint initiative of the Dutch universities to make all their research results digitally accessible"⁹².

11. Open questions and next steps in the development of trusted digital repositories

Trusted digital repositories present issues unique to the digital environment as well as issues encountered in more traditional repositories. In the last few years, great progress has been made in the intellectual and practical definition and realization of digital repositories and in the development of effective models that can be adopted and adapted by different institutions. The OAIS model has served as a catalyst, providing common ground for much research and helping the emergence of more unified approaches. Ongoing work is still required, though, in order to resolve many issues. The RLG/OCLC report recommends efforts towards certifi-

88 NEDLIB web-site available at: http://www.kb.nl/coop/nedlib (last accessed: 14 December 2004).

⁸⁹ See Oltmans and van Wijngaarden, Digital preservation in practice, pp. 21.

⁹⁰ See Digital Information Archiving System (DIAS), available at: http://www-5.ibm.com/nl/dias/index.html (last accessed: 14 December 2004). See also the related IBM / KB Long-term Preservation Study, available at: http://www-5.ibm.com/nl/dias/preservation2.html (last accessed: 14 December 2004).

⁹¹Robin Dale, electronic mail message to author, 13 October 2003. Wim van Drimmelen has underlined the importance of agreements with publishers: "Unlike printed publications, digital publications require from the publisher an active part in the archiving. Therefore arrangements with publishers are essential to realise the safe-keeping of the intellectual output of scientists;" in: Koninklijke Bibliotheek, News Archive, "National Library of the Netherlands and BioMed Central Agree to Open Access Archive" (press release, 17 September 2003) (available at: http://www.kb.nl/nieuws/2003/kbbiomed-en.html. Last accessed: 14 December 2004). Putting a system in place to safeguard publications, which the publishers may otherwise not preserve correctly, represents a proactive approach that aims at eliminating the risk of neglect. The 1996 report of the Commission on Preservation and Access/ RLG Task Force on Archiving of Digital Information discusses the "aggressive rescue function," that is, the right of digital archives to save digital information being neglected by its custodian (see Garrett and Waters, *Preserving digital information*: p. 40; also Robin Dale, electronic mail message to author, 13 October 2003).

⁹²DARE, Digital Academic Repositories, available at: http://www.surf.nl/en/themas/index2. php?oid=7 (last accessed: 14 December 2004). DARE was presented in session four of the ERPANET workshop on trusted digital repositories. See also the DAREnet web-site in English, available at: http:// www.darenet.nl/en (last accessed: 14 December 2004). The SURF web-site in English is available at: http://www.surf.nl/en/home/index.php (last accessed: 14 December 2004). cation, standardization and collaboration, and provides the following recommendations to organizations and institutions:

- Develop a process for the certification of digital repositories.
- Research and create tools to identify the significant attributes of digital materials that must be preserved.
- Research and develop models for cooperative repository networks and services.
- Develop systems for the unique, persistent identification of digital objects that expressly support long-term preservation.
- Investigate and disseminate information about the complex relationship between digital preservation and intellectual property rights.
- Determine the technical strategies that best provide for continuing access.
- Define the minimal-level metadata required for long-term management and develop tools to automatically generate and/or extract as much of it as possible⁹³.

These issues were also discussed at the ERPANET workshop on trusted repositories held in Rome in November 2003⁹⁴, along with the following open questions:

- Is it possible and/or necessary to agree on one definition of trusted digital repository?
- How do different communities see trusted digital repositories?
- What current implementations may be rightfully called "trusted digital repositories"?
- How are the concepts of reliability, authenticity and trustworthiness interpreted in different contexts and why?
- How should the roles and responsibilities of the many stakeholders be addressed?
- Is the potential of trusted digital repositories currently being adequately exploited?
- What issues have not yet been addressed in trusted digital repositories implementations and research?⁹⁵

93 RLG-OCLC, Trusted digital repositories, pp. i.

⁹⁴ ERPANET Workshop "Trusted repositories for preserving cultural heritage," Rome, 17-19 November 2003.

ERPANET web-site at: http://www.erpanet.org/events/2003/rome/index.php. Last accessed: 14 December 2004. <

⁹⁵ ERPANET, ErpaWorkshop: Trusted repositories for preserving cultural heritage. Final report, p. 5.

Work is currently being done in many of the areas listed above, for example in order to identify and establish ways to certify trusted digital repositories⁹⁶. RLG and the National Archives and Records Administration (NARA) have jointly created the Task Force on Digital Repository Certification; the task force's "purpose is to produce certification requirements for establishing and selecting reliable digital information repositories"⁹⁷.

Among other issues, at the Rome workshop Tito Orlandi has addressed the fact that it has not yet been clearly defined which characteristics of the records should exactly be preserved in the transition from the traditional to the digital environment⁹⁸.

At the workshop, the presentations of various initiatives (such as DSpace, LOCKSS, i-Tor, the ARELDA project, the activities of the National Archives of Australia, and more) and issues (such as the ones of repository design and creation, of digital voluntray deposit, and of metadata sets)⁹⁹ have shown different points of view and common concerns, in a constructive exchange of ideas among professionals and contexts. This kind of exchange is essential, now and in the future, in order to share solutions, avoid duplication of effort, and work together towards stable approaches.

⁹⁶ Robin Dale focused on certification in her presentation during session four of the ERPANET workshop on trusted digital repositories. An ERPANET Workshop on "Audit and Certification" was held in Antwerpen on 14-16 April 2004. See the web-site at: http://www.erpanet.org/events/2004/ant-werpen/index.php. Last accessed: 14 December 2004.

⁹⁷ RLG web-site, "Task Force on Digital Repository Certification" (available at: http://www.rlg. org/en/page.php?Page_ID=367. Last accessed: 14 December 2004).

⁹⁸ See ERPANET, ErpaWorkshop: Trusted Repositories for Preserving Cultural Heritage: 5-6. The requirements identified by the InterPARES 1 Project may help in this direction: see InterPARES Project-Authenticity Task Force, Requirements for Assessing and Maintaining the Authenticity of Electronic Records.

⁹⁹ See ERPANET, ErpaWorkshop: Trusted Repositories for Preserving Cultural Heritage. Final Report.

= INTERVENTI =

Ross HARVEY^A, Daisy ABBOTT^B, Brian AITKEN^B, Marlene VAN BALLEGOOIE^C, Christoph BECKER^D, Cecilia CASAS DESANTES^E, Volker HEYDEGGER^F, Yunhyong KIM^B, Leonidas KONSTANTELOS^B, Andrew MCHUGH^B, Stephan STRODL^D and Seamus ROSS^{B 1}

Emerging approaches for digital preservation in digital libraries: report on the Fifth DELOS International Summer School

Abstract: L'articolo costituisce un'accurata sintesi dei contenuti e dei risultati della quinta edizione della Delos International Summer School sulla conservazione digitale per le biblioteche e gli archivi digitali che quest'anno si è tenuta a San Miniato.

Abstract: The Fifth DELOS International Summer School on 'Digital preservation in digital libraries: emerging approaches' was held at the Centro Studi Cappuccini in San Miniato² from the 4-10 June 2006. The lectures aimed to assist the attendees to gain a coherent understanding of issues surrounding digital preservation within the context of digital library development and management, and introduce them to emerging research in the area of digital curation and preservation. Digital preservation is an area of research flux and a core curriculum has yet to emerge, so courses of this kind stimulate new kinds of research approaches and provide a valuable environment for professionals to keep up to date in the area. This paper describes the material that was covered in the course and in so doing sketches new directions for research.

^{1 a} Charles Sturt University, ^b HATII, University of Glasgow, ^c Toronto University Libraries, ^d Vienna University of Technology, ^e Museo Cerralbo, Ministerio de Cultura, España, ^f Universität zu Köln. All the authors of this report participated fully in its preparation. Ross Harvey ensured the overall intellectual consistency of the report. All the authors agreed the final version of the manuscript. While this is an objective report, it is not an independent evaluation of the Fifth DELOS International Summer School on 'Digital Preservation in Digital Libraries: Emerging Approaches' as the authors were all participants as either students or lecturers.

² Use of the Centro Studi i Cappuccini was made possible through the kindness of the Cassa di risparmio di San Miniato.