4th International Digital Curation Conference
December 2008

An Institutional Framework for Creating Authentic Digital Objects

Ronald Jantz
Digital Library Architect
Rutgers University Libraries

November, 2008

Abstract

In the future, a scholar or researcher will want to know that a digital object is trusted – that it is authentic and reliable. Digital objects can be surrogates, resulting from a digitization process, or they can be objects whose only form is digital. Much has been accomplished in existing open source digital library platforms to provide capabilities for preserving digital objects including now ubiquitous features such as persistent identifiers, integrity checks, audit trails, and versioning. However, achieving a level of digital object authenticity will require a multi-dimensional approach involving policies, processes, and continued technological innovation. This paper proposes steps the institution[1] can take to insure the availability of authentic digital objects in the future. In this proposal, authenticity is based on definitions from archival diplomatics and relies on methods from public key cryptography for digitally signing an object with a secure time stamp. Trustworthy processes, re-definition of traditional roles, and the implementation of technologies to support authenticity are all required to meet the needs of digital scholarship. Implementation and policy issues are discussed with specific attention to transformations required of the archival institution and the professional archivist.

[1] The term "institution" is used generically to refer to academic libraries, archival institutions, cultural heritage organizations or other non-profit information agencies involved in digital archiving.

The 4th International Digital Curation Conference taking place in Edinburgh, Scotland over 1-3 December 2008 will address the theme *Radical Sharing: Transforming Science?*.

Introduction

In his book on library history, Matthew Battles (2003, p. 212) expresses a vision of what digital objects might become: "The digital objects of today are the incunabula of a not-too-distant tomorrow – our palimpsests, our geniza bits, the refuse of our restless and inconsolable appetite for change and immortality". In discussing the information professional's role in preserving social memory, Owens (2003) illustrates, with poignant examples, how our cultural heritage resources have been destroyed over the last five millennia. He encourages librarians and archivists to develop the philosophical framework that encompasses the preservation of both print and electronic resources. In contrast to these digital surrogates, e-science introduces even more complexity with data-driven disciplines that are creating peta-scale datasets with many varied formats. As just one example, the archive for the Hubble Space Telescope project contains more than 27 terabytes of data and, as of year 2006, was growing at a rate of 390 gigabytes a month (Livio, 2006). In examining the transformation of roles, Sassoon (2007) indicates that archivists are still looking primarily at themselves for solutions and a more multidisciplinary approach is required in order to develop a "new regime of 21st century format specialists."

Each of these perspectives raises serious concerns about the risks inherent in digital research and scholarship and the roles required to support this type of scholarship. Scholarship is becoming increasingly digital – for some disciplines one might say that scholarship is exclusively digital. Relatively few of the digital resources in use today are given proper archival and preservation attention. Indeed, one might claim that 21st century scholarship depends on trusted methods for archiving and preserving digital information. Print artifacts lend themselves to various authentication techniques that are not available in the digital environment. Analysis of paper and ink provide clues about the provenance of handwritten documents. Scholars readily accept the date on a book that is provided by a trusted publisher. As in the print world, scholars want to know that they are working with authentic digital objects. We want to find corresponding attributes for digital material that can serve in lieu of these traditional markers.

Libraries and archival institutions are amassing large stores of digital information through their work with institutional repositories, grant-funded projects and digital publishing. As a consequence of these initiatives, they must also become competent digital archival institutions. These institutions must not only store these resources but they must also insure that digital information is trustworthy and persists for, hopefully, many hundreds of years. Digital content, being highly mutable, poses both technological and policy challenges for those institutions that undertake digital initiatives. How will institutions support scholarship that is increasingly based on digital resources? One can imagine that there are potentially many new services that can be offered and which are currently not part of the institutions' repertoire. This article elaborates on one such new service – the ability for a scholar or researcher to validate the authenticity of a digital object many years after the resource has been ingested into a digital repository.

Conceptual Frameworks

In addressing the objectives of this study, three perspectives are used – a) a three stage model for digital preservation and archiving, b) for authenticity and reliability, the science of archival diplomatics - and c) for the ever-present and

advancing technological framework, digital signatures and public key cryptography. It is proposed that the concepts within the science of diplomatics, specifically authenticity and reliability, can be transferred to the more general problems of archiving digital objects of any genre and preserving these objects in perpetuity.

A Three-Stage Model of Digital Archiving and Preservation

To provide the context for the remainder of this paper, some starting points are needed. The first is that the digital archiving and preservation process includes three major phases that proceed through time as depicted in Figure 1: digital capture and description, archiving and ingesting the object, and preserving the object over its life cycle.

Figure 1 – The Three-Stage Model

In each of the above phases, certain aspects of authenticity must be addressed as discussed in the following sections.

The Science of Diplomatics

Diplomatics concerns itself with the archival document or record in contrast to archival science which is typically concerned with aggregations of records (Duranti, Eastwood, & MacNeil, 2002, p. 10). Diplomatics originated in the 16th and 17th centuries when historians and lawyers wanted to date documents and assess the good faith and credibility of those who prepared documents (MacNeil, 2000). Diplomatics is concerned with the quality of a record, in particular the authenticity and reliability of the record and the possibility of attaching markers to the record that will help verify its authenticity and reliability. The approach in this article is to ask if we can apply these same concepts more generally to any digital object that is intended to be archived and preserved.

Public Key Cryptography

An internationally recognized method for meeting the requirements of authenticity is to create certificates by encrypting and digitally signing the source document. There are trusted mechanisms available today to digitally sign and date an object. The proposal herein is based on the research of Haber and Stornetta (1991), Haber, Kaliski, and Stornetta (1995), and Maniatus and Baker (2002). In public key cryptography, asymmetric techniques are used to encrypt a document using a private key. As part of a validation process, a public key can then be used to decrypt the document. The cryptographic transformation created with the private key can only be reversed using the public key. Digitally signing answers the question regarding identity, however the concept of time – when was the source document archived or modified – is also essential. Consequently, a method for producing a secure time stamp and associating it with the digital signature is also needed. Both Maniatus & Baker (2002) and Busey (2004) have outlined secure time stamp methods that can be implemented by the institution.

Authenticity

In what follows, operational definitions of authenticity are proposed that can work for both digital surrogates and born-digital objects. Duranti (2002, p. 23) has indicated that authenticity is a characteristic of all archival documents and it relates to the quality of the object. Authentic also implies that the document is genuine, it is what it claims to be, and it is reliable – the content can be trusted. The concepts of authenticity and reliability can have meaning within the more general frameworks of digital libraries and institutional repositories. As a first step, we want to associate the quality attributes of authenticity and reliability with the digital object as it is ingested into the archive. If this step is properly executed, a scholar or researcher will be able, at a later point in time, to verify the authenticity of the digital object.

An authentic digital object is what it claims to be. The obvious question is who is making the claims and how are they made? In the digital environment, there are typically two claimants involved in the creation of the digital object: the creator of the intellectual content – the scientist, scholar, author or person who stands for the authors and the archivist or creator of the metadata and the digital object. Within the archival institution, the person creating the digital object may be a cataloger, a digital curator, a special collections librarian, an archivist, a librarian subject specialist, or someone charged with the responsibility for long-term digital preservation. For rhetorical clarity in this article, this trained professional will be referred to as the archivist and the one who oversees the creation of the metadata and who can make a set of claims that are digitally signed using a trustworthy process. In stressing the need for fundamental changes, Ross (2005) proposes that the academic librarian is better suited than any other information intermediary to assume the role of a trusted third party. In Cullen's words (2000), ". . . a third party, ideally a trusted librarian, would put a marker on a digital object - a marker that could not be predicted or devised (guessed) – that would mark the document's time and date."

By digitally signing the object, the archivist is making the following three claims on behalf of the institution: a) metadata for the object has been created by an approved representative of the institution, b) the metadata is accurate and complete. Note that this does not include any claims as to the accuracy of the intellectual content of the resource, and c) the signer verifies that the digital object has been created and ingested using established trusted repository processes as documented by the institution's policies. These claims have both an institutional aspect and a professional aspect. The archivist is claiming, on behalf of the institution, that the 3-stage process, and specifically the digital signing process, is trustworthy. The archivist is also claiming, from a professional perspective, that he/she has determined, as best possible, that the digital object is what the metadata claims it to be. This claim is not only based on the professional skills of the claimant, but also on extensive liaison with the scholar including possibly face-to-face meetings and background research. Given this liaison activity, the creator of the intellectual content – the scholar or scientist – need not sign the source document, although this option remains open as a possible extension and would likely strengthen the authenticity claim.

Methods

We have discussed the meaning and semantics of authenticity as it might be interpreted for the generic digital object. In the discussion of methods, a distinction is made between legal and financial requirements and those of the scholarly community. To support scholarship, a primary archival function is to store the digital object safely

in the repository and, to be assured with an increased measure of trust, that the archival action took place at a certain point in time and by whom. If these characteristics of authenticity can be reliably implemented, digital scholarship will benefit immensely. Public key cryptography is used here to define a practical implementation of the concept of authenticity, including an institutional framework for creating a secure method for digitally signing and archiving a document. The institutional basis for this process requires the creation of a certificate authority (CA), an agency which issues digital certificates that authenticate the identity of organizations and individuals. Typically for legal and financial transactions, the CA is a commercial service organization, however, in this proposal, the certification functions are executed by the archival institution and thus the institution becomes its own certificate authority. The technical methods and underlying technology at work is known as asymmetric cryptography in which a private key is used for encryption and which is kept secure by the institution. A totally different key, the public key, is used to decrypt the signature.

A Scenario

Signing the Document

In a typical scenario, an archival service and a secure time stamping method will be needed (Maniatis & Baker, 2002). Given these technical prerequisites, the archival institution can take on the role of the certification authority. As such the CA creates and signs its own certificate and provides a certificate service to the archivist. The archivist registers with the CA and creates a public and private signing key, taking special precautions to keep the private key secure. The CA issues an identity certificate for the archivist with name, public key, and expiration date. Figure 2 illustrates a template for the archivist's certificate (Ford & Baum, 2000).

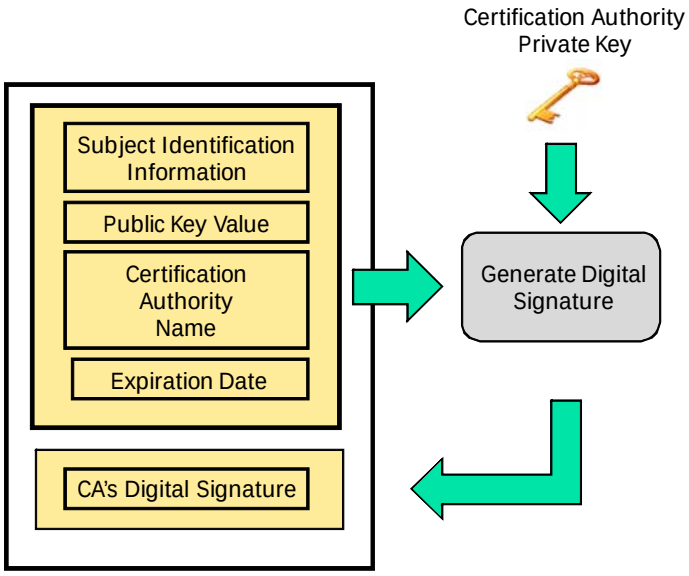

Figure 2 – A Typical Certificate

The archival master is the digital encoding of the document to be archived and is defined as the uncompressed, non-proprietary file or files in an open and standard format. One of these files must also include the metadata prepared by the archivist. To sign an archival master, the archivist executes the following steps which are illustrated

in Figure 3:

- In a liaison capacity, the archivist works with the researcher and encrypts the message digest of the document with the private key.
- The archivist submits the result to the time stamping service to acquire a secure time stamp.
- The encrypted message digest and time stamp are signed by the archivist and archived along with the archival master.

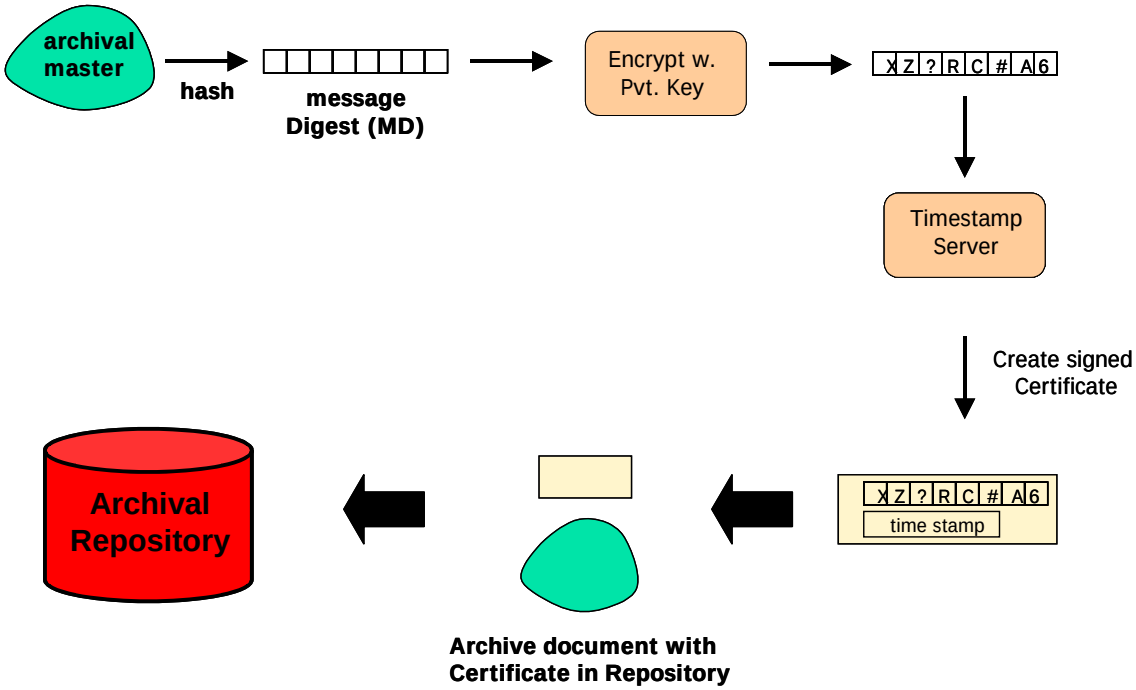

Figure 3 – The Signature and Time Stamping Process

Given the above procedures, at some later date a scholar can verify the authenticity of the digital object. The public key can be used to decrypt the message digest and determine if it is consistent with a re-computed message digest for the archival master. This step insures that the digital object has not been inadvertently modified. Further, via the certificate and the secure timestamp, the scholar can determine when the object was archived and the identity of the archivist. These verification steps are also dependent on the trust in the institution and trustworthy processes – a framework that is discussed in a later section.

Migration of the Document

A major part of life cycle management involves the migration forward of the archival master to new formats and standards. With the digital signing process, a new complexity is introduced into the migration process – managing signatures over the life cycle of the object. Haber and Kamat (2006) describe a process that builds on time stamping every document by also producing an auditable record of every transformation (migration) that is applied to the original document. The process enables one to verifiably link the time stamp certificate for the transformed document to the archival master that was first ingested. To outline this process, assume the archival master is migrated forward to a new format. According to Haber's approach, immediately after the migration, a new certificate is created that binds the original

master, the transformed master, the transformation algorithm, and the original certificate with a new time stamp. This process can obviously be repeated with successive migrations. On the surface, the approach might appear complex, however much of the technology has been worked out in a prototype implementation at Hewlett-Packard Laboratories (ibid, 2006). This procedure also suggests that the migration process must address the archiving of the transformation algorithm. This problem is endemic to the migration process and must be dealt with independently of the digital signing approach discussed here.

A Framework - The Institution and the Archivist

Much of the technology is available to establish a framework for creating authentic digital objects. For a practical realization of this framework, some important transformations are required of both the archival institution and the professional archivist. In this section, suggestions are put forward as to how to take steps within the institution to provide the capabilities for creating authentic digital objects. Academic libraries and similar institutions provide stable and persistent frameworks within academia and most users of libraries would claim that they are trusted institutions. This trust reputation is likely to be built on many years of service to the public in dealing with traditional, print-based materials. However, this tradition-based trust does not transform readily into trust in the digital environment. Scholars who study academic libraries have been pointing the community in the proper direction for several years. Atkinson (2005) states: "The library, by virtue of its most fundamental values and attributes, is probably better suited at this time than any other information intermediaries to assume such a role" [of a trusted third party]. He further states that the academic library will need to undertake some fundamental changes to assume this role of a trusted third party. In discussing the theoretical framework for knowledge acquisition, Budd (2004) stresses the role that librarians can play in the growth of knowledge and how the library can become the focus of a reliable process.

Trust in Information

A brief discussion of trust will provide a context for some of the fundamental changes to which Atkinson refers. To move ahead, it must be acknowledged that trust between the scholar and the institution will play a significant role. Societal models of trust emphasize that trust is important to the proper functioning of society (Kelton, et al; 2008) – a view that suggests that trust would also be important for scholarly communication. Trust is a complex, multi-faceted concept and can exist between individuals or an individual and an institution. In the model proposed by Panateli and Sockalingam (2005), there are three dimensions or stages of trust based on benefits, information, and identity. Information-based trust relies on researchers' – scientists and scholars – understanding of the processes and mechanisms that govern the creation of authentic digital objects. McDowell (2002) suggests that consumers – researchers in this context – must find ways to trust information in order to be confident in their acquisition of new knowledge. This type of trust is developed over time with repeated interactions between the user and the institution. In discussing trust, Kelton, et al (2008) have proposed a model that positions trust as a key mediating variable between information quality and information usage. The processes for developing trust can be organized into the following taxonomy: prediction, attribution, bonding, reputation, and identification. Of the five taxonomic characteristics identified by Kelton, attribution or dependability is a primary aspect of trust that the institution will need to

strengthen in order to become trusted. Attribution is based on the words, actions, and credible information of the trustee – "attribution is a cognitive process for assessing the trustee's competence, ethics, or other intentions" (ibid, 2008).

The Trusted Repository and the Certification Agent

Institutions such as academic libraries have built trust in their traditional services, however this trust does not yet exist in the digital domain. It is safe to say that that there are few institutions that can claim to having a trusted repository. The claims must be substantiated for trust to develop. The absence of standard procedures and quality controls inhibit the development of trust in an institution, a situation which is exacerbated by the necessity for life cycle curation and preservation. For an archivist to make a claim regarding the institution's trustworthy processes, these processes must be certified by an independent authority. It is not sufficient to make claims even when reliable and trustworthy processes are in place. The claims of being trustworthy must be open, transparent, and credible. To develop this credibility, an institution must look to a neutral, 3rd party to certify its processes for creating and managing authentic digital objects.

Certification of a repository is a major challenge and institutions have been slow to address this challenge. The concept of certification addresses an important need in the digital world. Certification falls short of a contract between the user and the library, however certification offers a much higher degree of openness and security than what exists today between the library and the user of digital resources. The *Trustworthy Repositories Audit and Certification: Criteria and Checklist*[2] (TRAC) provides an excellent starting point for this process, and the Center for Research Libraries[3] offers a service to member institutions to undergo certification. As illustrated in Figure 4, there are three major TRAC certification areas - organization, repository functions, and technical infrastructure – covering some 88 criteria. To illustrate how TRAC might apply to the procedures outlined here, a criterion is identified in each category of Figure 4 that relates to the scenario described earlier. For scholarly communication, it is important that the researcher understand the commitments made by the institution and, more specifically, the semantics and the process for creating authentic digital objects. This understanding can be facilitated through deposit agreements with the scholar (category A). As has already been discussed, delivering authentic objects is an essential function of the trustworthy repository. The actions required of the archivist in creating a certificate and signing the archival master would need to be covered under category B. Ultimately, we can only know that someone signed the document with a private key. The trust relationship has to provide the assurance that the document was in fact signed by the person identified in the signing certificate. These security issues would have to be covered under Category C, specifically those aspects of managing and keeping secure the private keys used by archivists.

In this author's opinion, for TRAC to better serve as an instrument in the certification process, three essential elements would have to be added: a) a quantitative metric that can indicate the relative importance of the criteria and can serve as a mechanism for measuring progress. Many institutions will not achieve certification on the first try and will need a more precise approach to measuring where they are and where they need to improve, b) a repeatable process for reviewing the institution's

[2] *Trustworthy Repositories Audit & Certification: Criteria and Checklist.* http://www.crl.edu/PDF/trac.pdf
[3] *Center for Research Libraries,* http://www.crl.edu/

credentials and to insure that they remain trusted year over year, and c) an official designation that the institution has been certified and which can be used to support the archivist's claims and establish credibility with the scholar. The Baldridge National Quality Program[4] offers a model which supports an iterative process of review, planning, and continuous improvement that is fundamental to institutional effectiveness. The Baldridge model is also being applied within academia to address an environment of rapid technological change (Furst-Bowe & Bauer, 2007). Part of the Baldridge continuing improvement process includes the assignment of point scores to major areas such as A, B, and C in Figure 4. By updating TRAC to address these extensions, trust in the attribution aspects of the repository can be strengthened and the archivist can cite an external authority to support claims of trustworthiness.

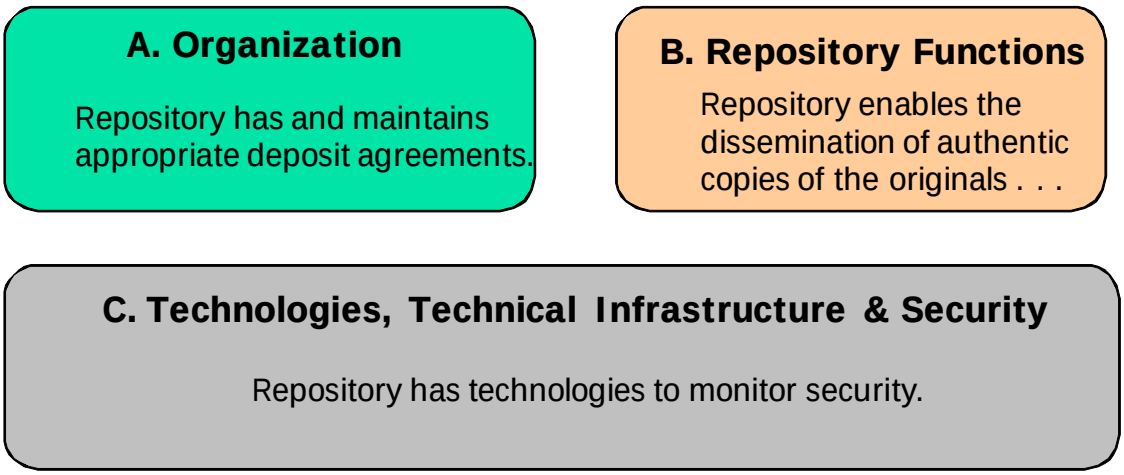

Figure 4 – TRAC Certification Areas

The Archivist - Transformed Roles and Skills

In an a special introduction issue on archiving research data, Doorn and Tjalsma (2007) comment that few information technologists are interested in digital preservation and that archivists and librarians must take the lead – "an understanding that is not yet shared by everybody." In a previous section of this article, tasks for the archivist and the librarian were outlined. Some readers may be inclined to interpret the digital archival role as technical and mechanical, however there are intellectual and professional connections that may not be so obvious. Within the context of the Certification Authority, librarians and archivists have the opportunity to leverage and transform their traditional skills. Anderson (2002) indicates that scholars are dependent on others in order to have their knowledge claims certified or rejected. The actions of creating an authentic digital object place the archivist in a key role as a cognitive authority in a trusted scholarly communication process.

As mentioned earlier, the archivist is charged with making a claim about the item to be authenticated. In e-science, the archivist, working in a liaison role, must be familiar with the scholarly processes used by scientists and be able to advise as to how to capture all relevant information needed to reproduce a scientific experiment. Wallace, et al (2007) stress the importance of extending archival practices upstream,

[4] *Baldrige National Quality Program*, http://www.quality.nist.gov/

capturing as much context and provenance as possible. An essential element of the liaison process is to insure completeness in the digital capture phase. In particular, have the essential elements of the experimental design been captured so that an experiment can be reliably repeated? This type of data is all too frequently omitted as is evidenced by the noteworthy cold fusion physics debacle (Adam, 2005). It should be further noted that the archival master as depicted in Figure 3 must also encapsulate all of the context and provenance that is captured as metadata. The liaison role and the preparation of authentic descriptive and technical metadata become essential ingredients of the digital signing process.

Discussion and Summary

This proposal is based on several assumptions as follows. First, the institution as a non-profit entity is likely to be more persistent than commercial certification and time stamping services. However, it must be acknowledged that institutions, servers, operating systems, and other technical components will come and go throughout the life cycle of the digital object. The preservation focus must continue to be on the data and the migration of data and signatures throughout these transitions. Authenticity is more narrowly defined for scholarly and research purposes which clears the way for implementing less costly solutions. Legal and financial issues are to be left to others. With these assumptions, the methods proposed here overcome the issues with digital signatures that have been ably summarized by Boudrez (2007).

Given the overhead of insuring authenticity, careful selection of digital objects must be exercised. Institutions should incorporate risk analysis in determining which digital objects require authenticity and they might start by applying this approach to born-digital objects that are used for scholarly and research purposes. Digital surrogates are typically at less risk since a corresponding physical artifact can usually be found. To minimize expense, institutions can also collaborate in a community of trust to share certification and time stamping services.

Many institutions are hesitant to incur the overhead implied by the processes outlined here. However, undergoing the certification process and providing a new service – creation of authentic digital objects – is not only necessary to support the integrity of scholarship, it is also offers the opportunity to extend traditional roles into the digital environment. As more digitization occurs, there are those who suggest that the only way academic librarianship will survive is for librarians “to invent replacement services for which they are uniquely qualified” (Gladney, 2008). Librarians and archivists appear to be uniquely qualified to take on this new service in collaboration with technologists who can provide the infrastructure support. Also, it should be noted that there are downstream institutional benefits that have been shown to accrue from those who have received the Baldridge Quality award. With proper trusted credentials, depositors will ultimately look to the archival institution as the rightful “place” for preservation and curation of their data, thus increasing deposits and usage of the institutional repository. An institutional management benefit also results from the certification process. Undergoing certification encourages introspection of the institutions’ practices for digital preservation, many of which are often insufficient. Certification by a 3rd party encourages the institution to examine its processes, prioritize, and focus on those areas that incur the most risk.

Credible digital scholarship requires authentic digital objects. Significant progress in both the technological and process domains suggests a convergence that will enable institutions to proceed with a digital signing service. To begin this work, the institution should address the following major areas:

- Develop the specific processes required of the certification authority
- Pursue certification as a trusted repository (e.g. by using TRAC)
- Establish the technical infrastructure for signing and time stamping by building on the existing methods and prototypes
- Assist personnel (librarians and archivists) to assume the role of creating authentic digital objects
- Collaborate with like-minded institutions to create a community of trust and share the cost of implementation

Ultimately, the institution and the scholar must recognize that the digital preservation community is dealing with probabilities. The approaches and technology outlined here offer the opportunity to significantly increase the probabilities of preserving the integrity of the digital object over time. Until further research uncovers more promising technologies, the authentic digital object will have to rely on human processes, imperfect and sometimes unreliable hardware and software, and a strong element of trust between the scholar and the institution. All of these will improve over time but we must begin the process. Information professionals and their institutions have an opportunity to re-interpret their roles in light of this rapidly changing technological environment in order to meet the challenges of creating authentic digital objects for research and scholarship.

References [use Style: "Reference-list-item"]

[journal article]Adam, D. (March/2005). In from the cold. *The Guardian.* Available at http://www.guardian.co.uk/education/2005/mar/24/research.highereducation2

[journal article]Anderson, J. (2002). The role of subject literature in scholarly communication: An interpretation based on social epistemology. *Journal of Documentation, 58,* (4), 463 – 481.

[journal article]Atkinson. R. (2005). Transversality and the role of the library as fair witness. *Library Quarterly, 75,* (2), 169 – 189.

[book]Battles, M. (2003). *Library: An Unquiet History.* New York: W.W. Norton and Company.

[journal article]Boudrez, F. (2007). Digital signatures and electronic records. *Archival Science, 7,* 179 – 193.

[journal article]Budd, J. (2004). Academic libraries and knowledge: A social epistemology framework. *Journal of Academic Librarianship, 30,* (5), 361 – 367.

[report]Busey, J. (2004). A proposal for distributed digital time-stamping. Available at: http://ww2.cs.fsu.edu/~busey/samplework/DigitalTimestamping.pdf. Accessed July 9, 2008.

[journal article]Cullen, C. (2000). Authentication of digital objects: Lessons from a historian's research. In: *Authenticity in a Digital Environment,* pp. 1 – 7. Available at: http://www.clir.org/PUBS/reports/pub92/pub92.pdf . Washington, DC: Council of Library and Information Services

[journal article]Doorn, P. & Tjalsma, H. (2007). Introduction: archiving research data. *Archival Science, 7,* 1 –20.

[book]Duranti, L., Eastwood, T., & MacNeil, H. (2002). *Preservation of the Integrity of Electronic Records.* Dordrecht, Boston, London: Kluwer Academic Publishers.

[book]Ford, W. & Baum, M. (2000). *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption,* 2nd Edition, Upper Saddle River, NJ: Prentice Hall PTR.

[journal article]Furst-Bowe, J. & Bauer, R. (2007). An application of the Baldridge model for innovation in higher education. *New Directions for Higher Education, 137,* 5 – 14.

[journal article]Gladney, H. (2008). Perspectives on trustworthy information: Marginalization of research libraries. *Digital Document Quarterly, 7,* (1). Retrieved May 11, 2008 from http://home.pacbell.net/hgladney/ddq_7_1.htm

[proceedings]Haber, S. & Kamat, P. (2006). A content integrity service for long-term digital archives. *Proceedings of the 2006 Imaging Science & Technololgy Conference,* Ottawa, Canada, May 23 – 26, 2006.

[journal article]Haber, S., Kaliski, B., & Stornetta, W. (August/1995). How do digital time-stamps support digital signatures? *Cryptobytes, RSA Laboratories 1,* (3), 14 – 15.

[journal article]Haber, S. & Stornetta, W. (1991). How to time-stamp a digital document. *Journal of Cryptology: The Journal of the International Association for Cryptologic Research, 3,* (2), 99 – 111.

[journal article]Kelton, K., Fleischmann, K. & Wallace, W. (2008). Trust in digital information. *Journal of the American Society for Information Science and Technology, 59,* (3), 363 – 374.

[journal article]Livio, M. (July/2006). Hubble's top 10. *Scientific American, 27 – 32.*

[book]MacNeil, H. (2000). *Trusting Records: Legal, Historical, and Diplomatic Perspectives.* Dordrecht, Boston, London: Kluwer Academic Publishers.

[proceedings]Maniatis, P. & Baker, M. Enabling the archival storage of signed documents. *Proceedings of the FAST 2002 Conference on File and Storage Technologies,* Monterey, California, January 28-30, 2002.

[journal article]McDowell, A. (2002). Trust and information: The role of trust in the social epistemology of information science. *Social Epistemology, 16,* (1), 51 – 63.

[journal article]Owens, B. (2003). The safeguarding of memory: The divine function of the librarian and archivist. *Library & Archival Security, 18,* (1), 9 – 41.

[journal article]Panateli and Sockalingam (2005). Trust and conflict within virtual inter-organizational alliances: a framework for facilitating knowledge sharing. *Decision Support Systems, 39,* (4), 599 – 617.

[journal article]Sassoon, J. (2007). Beyond chip monks and paper tigers: Towards a new culture of archival format specialists. *Archival Science, 7,* 133 – 145.

[journal article]Wallace, J., Borgman, C., Mayernik, M., & Pepe, A. (2008). Moving archival practices upstream: An exploration of the life cycle of ecological sensing data in collaborative field research. *The International Journal of Digital Curation, 1,* (3), 114 – 126.

[proceedings]Yamaji, K., Kataoka, T., Sonehara, N., & Namiki, T. (2008). Time stamping preprint server environment using Eprints 3. Poster session. Available at: http://pubs.or08.ecs.soton.ac.uk/77/ *The Third International Conference on Open Repositories, Southampton, UK, April 1 – 4, 2008.*