Canadian Conservation Institute

Institut canadien de conservation

Preservation of Electronic Records: New Knowledge and Decision-making

La préservation des documents électroniques : Information récente et prise de décisions

Canadian Heritage | Patrimoine canadien

Canada

Table of Contents/Table des matières

Foreword

The preservation of electronic records is one of the latest challenges facing the conservation and heritage communities. It is a complex and multifaceted task that includes content, media, hardware, and software.

The program for *Symposium 2003 - Preservation of Electronic Records: New Knowledge and Decision-making* was developed to deal systematically and logically with the various issues. The organizing partners — the Canadian Conservation Institute (CCI), Library and Archives Canada (LAC), and the Canadian Heritage Information Network (CHIN) — all have extensive experience in the field of electronic record preservation, and each brought a unique perspective on specific aspects of the topic.

But the challenge of preserving electronic records extends well beyond the traditional heritage community. It really includes all custodians of electronic information — from corporations to government agencies to individuals. To meet this need, the symposium also included a separate half-day event for the general public.

The organizing partners were delighted to welcome more than 350 delegates to the symposium; of these, 85% were from Canada, 10% from the United States, and the rest from a variety of countries including Australia, Bermuda, the Cayman Islands, Cuba, France, Italy, Malaysia, Mexico, the Netherlands, New Zealand, Taiwan, and the United Kingdom. Everyone participated actively in the discussions, and returned to their institutions with not only a better understanding of the challenges but also with viable and practical solutions that can be implemented immediately.

Charles Costain
Acting Director General
Canadian Conservation Institute (CCI)

Ian E. Wilson
National Archivist
Library and Archives Canada (LAC)

Roch Carrier
National Librarian
Library and Archives Canada (LAC)

Jean-Marc Blais
Acting Director General
Canadian Heritage Information Network (CHIN)

Avant-propos

La préservation des documents électroniques compte parmi les plus récents défis que doivent relever les collectivités de la conservation et du patrimoine. Cette tâche complexe concerne de nombreux éléments tels que le contenu, les médias, le matériel et les logiciels.

L'objectif du programme du *Symposium 2003 – La préservation des documents électroniques : Information récente et prise de décisions* est de se pencher systématiquement et logiquement sur les divers enjeux. Les organisateurs partenaires – l'Institut canadien de conservation (ICC), Bibliothèque et Archives Canada (BAC) et le Réseau canadien d'information sur le patrimoine (RCIP) – possèdent tous une vaste expérience de la préservation des documents électroniques, et chacun d'entre eux apporte un éclairage unique à des aspects précis de la question.

Mais le défi que représente la préservation des documents électroniques dépasse de loin la collectivité du patrimoine. Il inclut en fait tous les détenteurs de renseignements électroniques – des sociétés aux organismes gouvernementaux, et jusqu'aux particuliers. En vue de satisfaire ce besoin, une activité d'une demi-journée à l'intention du grand public fut présentée dans le cadre du symposium.

Les organisateurs partenaires ont été ravis d'accueillir plus de 350 participants, dont 85 % venaient du Canada, 10 % des États-Unis et 5 % de divers pays y compris l'Australie, les Bermudes, les îles Caïmans, Cuba, la France, l'Italie, la Malaisie, le Mexique, les Pays-Bas, la Nouvelle-Zélande, Taïwan et le Royaume-Uni. Tous ont pris part activement aux discussions, et tous sont retournés dans leurs établissements avec non seulement une meilleure compréhension des défis à relever, mais également avec des solutions pratiques qu'ils seront en mesure de mettre en œuvre sur-le-champ.

Charles Costain
Directeur général par intérim
Institut canadien de conservation (ICC)

Ian E. Wilson
Archiviste national du Canada
Bibliothèque et Archives Canada (BAC)

Roch Carrier
Administrateur général/ Bibliothèque nationale du Canada
Bibliothèque et Archives Canada (BAC)

Jean-Marc Blais
Directeur général par intérim
Réseau canadien d'information sur le patrimoine (RCIP)

Organizing Committee

Co-Chairs: Jane Down (CCI), Mary Murphy (LAC), Richard Green (LAC), Pat Young (CHIN)

Program: Joe Iraci (CCI) (*Chair*), Tom Strang (CCI), René Paquet (LAC), Bruce Walton (LAC), Gilles St-Laurent (LAC), Fay Hjartarson (LAC), Sheila Carey (CHIN)

Posters: Wanda McWilliams (LAC) (*Chair*), Alison Bullock (LAC), Janet Mason (CCI), Greg Hill (LAC), Bonnie Szirtes (CHIN)

Publications/Signs: Barbara Patterson (CCI) (*Chair*), Linda Leclerc (CCI), Sophie Georgiev (CCI)

Tours: Mary-Lou Simac (CCI) (*Chair*), Brenda Muir (LAC), Mike Thompson (LAC), Denis Gagnon (LAC)

Preservation Quest: Linda Street (CCI) (*Chair*), Joe Iraci (CCI), Lise Perron-Croteau (CCI), Carol MacIvor (CCI), Shanna Ramsay (CCI), Yvette Hackett (LAC), Louisa Coates (LAC), Randall Ware (LAC), Chris Dicks (LAC), Paul Lima (CHIN), Jane Down (CCI), Greg Hill (LAC)

Local Arrangements: Greg Hill (LAC) (*Chair*), Katherine Phillips (LAC), Natalie Labonté (LAC), Judith Falardeau (LAC), Colette Landry (CCI)

Trade Show/Marketing: Shanna Ramsay (CCI) (*Chair*), Chris Dicks (LAC)

Registration/Correspondence: Christine Bradley (CCI) (*Chair*)

Finance: Colette Landry (CCI) (*Chair*)

Media Relations: Carol MacIvor (CCI) and Louisa Coates (LAC) (*Co-Chairs*), Pauline Portelance (LAC), Paul Lima (CHIN), Shanna Ramsay (CCI)

Comité organisateur

Coprésidents : Jane Down (ICC), Mary Murphy (BAC), Richard Green (BAC), Pat Young (RCIP)

Programme : Joe Iraci (ICC) (*président*), Tom Strang (ICC), René Paquet (BAC), Bruce Walton (BAC), Gilles St-Laurent (BAC), Fay Hjartarson (BAC), Sheila Carey (RCIP)

Affiches : Wanda McWilliams (BAC) (*présidente*), Alison Bullock (BAC), Janet Mason (ICC), Greg Hill (BAC), Bonnie Szirtes (RCIP)

Publications/Panneaux : Barbara Patterson (ICC) (*présidente*), Linda Leclerc (ICC), Sophie Georgiev (ICC)

Visites : Mary-Lou Simac (ICC) (*présidente*), Brenda Muir (BAC), Mike Thompson (BAC), Denis Gagnon (BAC)

À la sauvegarde de votre patrimoine : Linda Street (ICC) (*présidente*), Joe Iraci (ICC), Lise Perron-Croteau (ICC), Carol MacIvor (ICC), Shanna Ramsay (ICC), Yvette Hackett (BAC), Louisa Coates (BAC), Randall Ware (BAC), Chris Dicks (BAC), Paul Lima (RCIP), Jane Down (ICC), Greg Hill (BAC)

Organisation locale : Greg Hill (BAC) (*président*), Katherine Phillips (BAC), Natalie Labonté (BAC), Judith Falardeau (BAC), Colette Landry (ICC)

Salon commercial/Promotion : Shanna Ramsay (ICC) (*présidente*), Chris Dicks (BAC)

Inscription/Correspondance : Christine Bradley (ICC) (*présidente*)

Finances : Colette Landry (ICC) (*présidente*)

Relations avec les médias : Carol MacIvor (ICC) et Louisa Coates (BAC) (*coprésidentes*), Pauline Portelance (BAC), Paul Lima (RCIP), Shanna Ramsay (ICC)

Acknowledgements

The hosting partners would like to extend their thanks to the Organizing Committee and all volunteers, speakers, poster presenters, session chairs, exhibitors, and sponsors, including the following organizations:

Audio Conservation Studio of Library and Archives Canada
Audio Visual Preservation Trust
Gatineau Preservation Centre
Canada Museum of Science and Technology
Canadian Conservation Institute
Canadian Heritage Information Network
Canadian Museum of Civilization
Department of Canadian Heritage
Library and Archives Canada
The Willow Group
Translation Bureau, Public Works and Government Services Canada
Tunstall & Tunstall Data Recovery Services

Remerciements

Les partenaires hôtes désirent remercier le Comité organisateur et tous les bénévoles, les conférenciers, les personnes qui ont présenté des affiches, les présidents de séances, les exposants et les commanditaires, y compris les organismes suivants :

Bibliothèque et Archives Canada
L'Institut canadien de conservation
Le Bureau de la traduction, Travaux publics et Services gouvernementaux Canada
Le Centre de préservation de Gatineau
Le ministère du Patrimoine canadien
Le Musée canadien des civilisations
Le Musée des sciences et de la technologie du Canada
Le Réseau canadien d'information sur le patrimoine
Le studio des enregistrements sonores de la Division de la musique (Bibliothèque et Archives Canada)
Le Trust pour la préservation de l'AV
Tunstall & Tunstall Data Recovery Services
The Willow Group

Preface

Symposium 2003 - Preservation of Electronic Records: New Knowledge and Decision-making took place in Ottawa on September 15–18, 2003, with a program that took the form of a decision tree. Following this format, the sessions could focus on areas that related to each other in a structured manner and all the key issues relating to the preservation of electronic records could be introduced in a logical sequence from the opening to closing speakers. The topics discussed included not only storage media but also the issues that must be addressed before considering how long an electronic record will last. [For the purpose of this symposium, the term "electronic record" was used to describe a large variety of records, e.g. audio and video recordings in analog or digital form and data files such as text, spreadsheets, e-mails, etc.]

The decision tree was initially formulated by the Program Committee, but refined by Tom Strang from CCI and Bruce Walton from LAC. Addressing the key decisions/choices that an institution needs to make when considering the acquisition and preservation of electronic records led to five main session categories: Appraisal of Electronic Records; Authenticity of Electronic Records; Developing a Preservation Strategy for Electronic Records; Preservation Strategies for Electronic Records; and Media Knowledge. The call for papers clearly outlined this approach, and resulted in the submission of more than 45 abstracts. Because of the decision tree program structure, the process to select the papers was very specific. The final program consisted of 29 papers from 6 countries: Canada (14); United States (8); Australia (3); United Kingdom (2); France (1); and Germany (1). In addition to the main program, 4 posters that fit into the program structure were also presented (1 from Canada, 2 from the United States, and 1 from France).[1]

Another objective of the program was to feature a wide variety of small- to medium-sized institutions that included not only archives and libraries, but also cultural institutions such as art galleries and museums that are faced with preserving electronic records. For example, art galleries often include video art in their collections, but the needs of these electronic records are quite different than the needs

1. One of the posters that was presented at the symposium was the decision tree that appears on p. 2 of the "Introduction" of this book of postprints. Hence, only three abstracts are included in the "Posters" section.

Préface

Symposium 2003 – La préservation des documents électroniques : Information récente et prise de décisions a eu lieu à Ottawa, du 15 au 18 septembre 2003, avec un programme qui a pris la forme d'un arbre de décision. Selon ce format, les séances pouvaient porter sur des sujets liés entre eux de façon structurée et tous les points importants concernant la préservation des documents électroniques pouvaient être présentés logiquement, du premier au dernier conférencier. Les sujets discutés incluaient non seulement les supports de préservation, mais aussi les questions à traiter avant de se demander quelle est la durée de vie d'un document électronique. [*Nota* : Pour les fins de ce symposium, le terme « document électronique » a été utilisé pour désigner un large éventail de documents, comme les enregistrements audio et vidéo sous forme analogique ou numérique et les fichiers de données tels que les textes, les tableurs, les courriels, etc.]

L'arbre de décision a d'abord été formulé par le comité du programme et raffiné ensuite par Tom Strang, de l'ICC, et Bruce Walton, de BAC. Les choix les plus importants que doit faire une institution et les décisions clés qu'elle doit prendre au moment de penser à l'acquisition et à la préservation des documents électroniques ont mené à l'établissement de cinq catégories principales de séances : Évaluation des documents électroniques; Authenticité des documents électroniques; Élaboration d'une stratégie de préservation des documents électroniques et Connaissance des supports. Cette approche a été soulignée dans la demande de communications, et plus de 45 résumés ont été soumis. Grâce à la structure du programme en arbre de décision, le processus de sélection a été très précis. Le programme final a consisté en 29 communications représentant six pays : le Canada (14); les États-Unis (8); l'Australie (3); le Royaume-Uni (2); la France (1) et l'Allemagne (1). En plus du programme principal, quatre affiches qui cadraient avec la structure du programme furent également présentées (une du Canada, deux des États-Unis et une de la France).[1]

Un autre objectif du programme consistait à présenter une grande variété de petites à moyennes institutions possédant non seulement des archives et des

1. Une affiche présentée au symposium portait sur l'arbre de décision qui apparaît à la page 2 de l'introduction du présent ouvrage. Par conséquent, seules trois affiches font partie de la section sur les affiches.

of the electronic records typically found in archives and libraries. Thus, the speakers list included several individuals from the museum and gallery communities.

Finally, it was important that the program include some case histories that highlighted what various institutions have actually done or are doing to preserve electronic records. While discussing preservation strategies is important, seeing strategies actually being implemented and working in the real world provides useful information and models to follow. Among the case histories presented were the preservation of audio language recordings from Aboriginal elders in the Northwest Territories in Canada, the preservation of American poet Robert Creeley's computer files, and the implementation of the Victorian Electronic Records Strategy (VERS) within the Government of the State of Victoria, Australia. The case histories were arguably the most useful aspect of a program that included something for everyone.

As a whole, the program provided delegates with a sense of the broader issues involved in collecting and preserving electronic records, as well as knowledge about the challenges that other institutions are facing and how they are dealing with them.

We are pleased to present the papers from the symposium program in this book of postprints. However, because speakers were given the opportunity to revise their papers after the symposium and the final submissions were lightly edited, the text herein may differ slightly from the original presentations.

Jane Down, CCI
Richard Green, LAC
Joe Iraci, CCI
Mary Murphy, LAC
Patricia Young, CHIN

Note: The papers in this book are published in the language in which they were presented, but all include an abstract in both English and French.

bibliothèques, mais aussi des institutions culturelles telles que des musées qui doivent conserver des documents électroniques. Les musées, par exemple, incluent souvent de l'art vidéo dans leurs collections, mais les besoins de consultation de ces documents électroniques sont bien différents de ceux qu'on retrouve habituellement dans les archives et les bibliothèques. Ainsi, la liste des conférenciers comprenait plusieurs personnes du monde muséal.

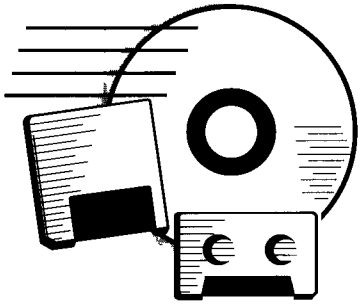
Enfin, il était important de retrouver dans le programme des histoires de cas afin d'illustrer ce que diverses institutions ont fait ou font concrètement pour préserver leurs documents électroniques. La discussion des stratégies de préservation est certes importante, mais le fait de connaître des stratégies qui sont mises en œuvre et qui fonctionnent dans une situation réelle permet d'obtenir de l'information utile et d'avoir des modèles à suivre. Parmi les cas décrits, il y a eu la préservation des enregistrements sonores des aînés autochtones des Territoires du Nord-Ouest, au Canada, la préservation des fichiers informatiques du poète américain Robert Creeley et la mise en application de la stratégie VERS pour les documents électroniques de l'État de Victoria, en Australie. On peut soutenir que les cas présentés formaient l'aspect le plus utile d'un programme répondant aux attentes d'un grand nombre de participants.

En général, les délégués sont repartis avec une vue d'ensemble des grandes questions liées à la collection et à la préservation des documents électroniques de même qu'une connaissance des problèmes auxquels se heurtent d'autres institutions ainsi que de leur manière de les résoudre.

Nous sommes fiers de vous présenter les communications du symposium dans cet ouvrage. Cependant, étant donné que les conférenciers ont eu l'occasion de modifier leurs textes après le symposium et qu'ils ont été légèrement révisés, il est possible que les textes soient quelque peu différents de ceux présentés durant le symposium.

Jane Down, ICC
Richard Green, BAC
Joe Iraci, ICC
Mary Murphy, BAC
Patricia Young, RCIP

Remarque : les communications sont publiées dans la langue utilisée lors de la présentation, mais toutes sont accompagnées d'un résumé en français et en anglais.



Authenticity Requirements for Electronic Records

Luciana Duranti

School of Library, Archival and Information Studies
University of British Columbia
#831-1956 Main Mall
Vancouver BC V6T 1Z1
Canada
Tel.: (604) 822-2587
E-mail: luciana@interchange.ubc.ca

Abstract

If electronic records are ever to be as trustworthy as records on traditional media, the practices by which they are created, maintained, and used must be analysed, and strategies and standards for their authentic preservation must be developed. This was the mission of a project known as InterPARES (International Research on Permanent Authentic Records in Electronic Systems), which has developed two sets of authenticity requirements for administrative records generated or maintained in databases or document management systems: Benchmark Requirements Supporting the Presumption of Authenticity of Electronic Records, and Baseline Requirements for the Production of Authentic Copies of Electronic Records. A second phase of InterPARES has begun studying the applicability of such requirements to interactive, dynamic, and experiential records produced by artistic, scientific, and e-government activities. This paper presents the requirements for authenticity and discusses the challenge posed to their application by the complexity of new types of digital records.

Introduction

In 1922, Sir Hilary Jenkinson identified "authenticity" as one of the characteristics of archival material, and linked it to the procedures of their creation, maintenance, and preservation. Archival documents are trustworthy as statements of fact because those who generate them need to rely on them for action or reference, and they are trustworthy as records because that same need of the creator and its legitimate successor(s) ensures that proper guarantees are put into place to keep them intact over time, both in the short and the long term.[1] With electronic records, however, a presumption of authenticity based on the reliance on them by their creator and on continuous unbroken custody is no longer possible. Because of their manipulabilty, vulnerability, and fragility, the authenticity of electronic records is constantly at risk, especially when they are transmitted across space and time and when they are migrated from an obsolete system to a new one. Thus, authenticity cannot be considered a characteristic of all electronic records, but only of those whose processes of creation, maintenance, and preservation respect certain pre-established requirements aimed at the protection of their authenticity. In all other cases, authenticity must be verified.

Between 1999 and 2001, the InterPARES[2] project identified and articulated requirements that would ensure the protection and permanent preservation of the authenticity of electronic records generated or maintained in databases or document management systems. It did so on the basis of concepts rooted in the traditional disciplines of diplomatics and archival science and elaborated and refined in light of the characteristics of contemporary records. In fact, in order to develop authenticity requirements for electronic records, the InterPARES research team determined that it was necessary to establish what a record was, at least as a hypothesis that the actual investigation could support or overturn. The team decided to adopt the definition of a "record" as any document created (i.e. made or received and set aside for further action or reference) by a physical or juridical person in the course of a practical activity as an instrument and byproduct of it, thereby choosing the traditional archival concept over the traditional diplomatic one, according to which a record is written evidence of a juridical fact. The team then proceeded to define "document" as recorded information, "information" as a message intended for communication across space or time, and "data" as the smallest meaningful piece of information. Finally, an "electronic record" was defined as a record created (i.e. made or received and set aside for action or reference) in electronic form, meaning that a message received in electronic form but set aside for action in paper form is a paper record, while a letter

received on paper but scanned in the computer and only used as a digital file is an electronic record. However, the research focused on records born, maintained, and used in electronic form.

Regardless of the choice of an archival definition for an electronic record, diplomatics (the science developed in the 17th century for the purpose of ascertaining the authenticity of records attesting patrimonial and personal rights) was essential to determining the necessary characteristics of such records. The following characteristics were identified:

- a fixed form, meaning that the binary content of the record must be stored so that it remains complete and unaltered, and its message can be rendered with the same documentary form it had when first set aside
- an unchangeable content
- explicit linkages to other records within or outside the digital system, through a classification code or other unique identifier
- an identifiable administrative context
- an author, an addressee, and a writer
- an action, in which the record participates or which the record supports either procedurally or as part of the decision-making process

The other concept that needed to be clarified was that of "authenticity," which was defined as the trustworthiness of the record as a record. In other words, the term refers to the fact that a record is what it purports to be and has not been tampered with or otherwise corrupted. Authenticity differs from authentication, which is one of the means used to prove that a record is authentic at a given moment in time. To understand further what the idea of authenticity implies with regard to its existence and preservation, the research team divided the concept into two components: identity and integrity. Identity refers to the attributes of a record that uniquely characterize it and distinguish it from other records, such as its date and the names of the persons involved in its formation. Integrity is the wholeness and soundness of a record. A record has integrity if it is intact and uncorrupted, i.e. if the message that it is meant to communicate in order to achieve its purpose is unaltered. This means that a record's physical integrity, such as the proper number of bit strings, may be compromised, provided that the articulation of the content and its required elements of form remain the same.

Authenticity requirements

On the basis of these concepts, the team developed two sets of authenticity requirements. The first set, called "Benchmark Requirements," is meant to support the presumption of the authenticity of the electronic records of a creator before they are transferred to the custody of the preserver. The presumption of authenticity is an inference that is drawn from known facts about the manner in which a record has been created and maintained, and is based upon the number of requirements that have been met and the degree to which each has been met. The second set, called "Baseline Requirements," is meant to support the production of authentic copies of electronic records that have been transferred to the custody of the preserver. The two sets of requirements are based respectively on the notions of a trusted record-keeping system and trusted custodianship. A trusted record-keeping system is one that controls what records are included in the system; who can include, retrieve, modify, delete, or remove them from the system; and how the records are included, maintained, retrieved, deleted, or removed from the system. A trusted custodian is a person entrusted with the responsibility of preserving the records — someone who has demonstrated that they have no reason to alter the records entrusted to their care or to allow others to do so, and who is capable of implementing the necessary measures for the physical and intellectual protection of the records.

Benchmark requirements

There are eight Benchmark Requirements: the first identifies the fundamental information about an electronic record that establishes its identity and allows for the demonstration of its integrity; the other seven identify the types of procedural controls over the record's creation, handling, and maintenance that support a presumption of integrity. In contrast to the Baseline Requirements (which are based on archival science), all Benchmark Requirements are derived from the diplomatic body of knowledge.

Benchmark Requirement 1 — The first requirement prescribes that the value of the following attributes[3] are explicitly expressed and inextricably linked to every record. These attributes can be distinguished into categories, the first concerning the identity of records and the second concerning the integrity of records:

A.1.a Identity of the record:

A.1.a.i Names of the persons concurring in the formation of the record, i.e. name of author, writer, originator, and addressee

A.1.a.ii Name of action or matter

A.1.a.iii Date(s) of creation and transmission: chronological date, received date, archival date, transmission date(s)

A.1.a.iv Expression of archival bond
A.1.a.v Indication of attachments
A.1.b Integrity of the record:
A.1.b.i Name of handling office
A.1.b.ii Name of office of primary responsibility
A.1.b.iii Indication of types of annotations added to the record
A.1.b.iv Indication of technical modifications

These attributes may appear as elements of record form or as annotations on the face of the record (e.g. the date, the name of the handling office), but they are more likely to be metadata linked to the record. It is essential that these attributes be inextricably linked to the record. This means that their presence in separate parts of the system, such as the audit trail, is not only unpractical (because the preserver would have to maintain a very large amount of unneeded information in order to keep the specific data related to a record), but it is not helpful in guaranteeing their permanent accessibility in connection with the record and their ongoing existence. The two primary means of linking these attributes to a record are the record profile and the topic map. A record profile is a form inextricably linked to a record, which includes specific fields for the automatic or manual inclusion of data related to the record; it is very common in electronic records management systems. A topic map visually expresses the characteristics of a record and the relationships among them. Whenever a record is removed from the system for external storage, migrated on the occasion of a system upgrade, or transferred to the preserver, the attributes must go with it, remain inextricably linked to it, and be accessible to the user.

Benchmark Requirement 2 — The second requirement regards access privileges. It prescribes that a presumption of authenticity be supported by the fact that the creator has defined and effectively implemented access privileges concerning the creation, modification, annotation, relocation, and destruction of records. The assignment of the authority and capacity to carry out administrative action on the records must therefore be accompanied by the exclusive technical capability to exercise such responsibility. This is usually done by creating, inside the system, tables of users' profiles that provide differentiated kinds of access depending on the users' administrative competence. However, access control can also be exercised by means of external security systems, such as the exclusive assignment of a key to a location. The effective implementation of access privileges consists of monitoring access through the use of audit trails that record each interaction of a user with a record.

Benchmark Requirement 3 — The third requirement prescribes that the creator has established and implemented procedures to prevent, discover, and correct loss or corruption of records. Examples of these procedures include the making of regular backups of records and their attributes, as well as of the entire system; and ensuring that the backup and recovery procedures will guarantee that, in the event of system failure, all complete updates are reflected in the rebuilt files as are any incomplete operations.

Benchmark Requirement 4 — The fourth requirement prescribes that the creator has established and implemented procedures to guarantee the continuing identity and integrity of records against media deterioration and across technological change. To counteract media fragility and technological obsolescence, the creator must plan upgrades to the technological infrastructure of its organization, making sure that the ability to retrieve, access, and use records when the upgrades occur is maintained. In addition, the creator must plan procedures of refreshment of the records, moving them from one storage medium to another, and of migration of the records from obsolescent to new technologies.

Benchmark Requirement 5 — The fifth requirement prescribes that the creator has established the documentary forms of records associated with each procedure either according to the requirements of the juridical system or those of the creator. This requirement derives from the fact that the authors of electronic records feel much freer in their compilation than the authors of paper records, and tend to let the technology, rather than administrative procedure, determine the form of the record. An acceptable compromise is to let the documentary form of a record be determined by workflow control technology, where one can connect each step of a procedure to a documentary form. Also, the creator can customize specific applications for the whole organization, so that all e-mails or all spreadsheets of a certain kind, for example, will present the same form. The control on documentary form must go down to the level of record elements, because this is the level at which the authenticity of the record is maintained and can be verified.

Benchmark Requirement 6 — The sixth requirement prescribes that, if authentication is required by the juridical system or the needs of the organization, the creator has established specific rules regarding which records must be authenticated, by whom, and by what means of authentication. This requirement may be met by linking the authentication of specific types of records to the various steps of the administrative

procedure, assigning responsibility to a given officer or an office for authenticating either individual or all records, and determining either a method of authentication valid for the entire organization or specific authenticating instruments for specific types of records.

Benchmark Requirement 7 — The seventh requirement prescribes that, if multiple copies of the same record exist, the creator has established procedures that identify which record is authoritative. One of the greatest problems presented by electronic records is the easiness of reproduction. Innumerable copies of each record may exist in an organization, each copy slightly different from the others either because it resides in a different hard drive of a different computer or because it has modifications voluntarily applied to it by various persons in the organization. It is vital for an organization to know which record is the official one, especially because each instance of the same record is inevitably a copy, either of an original or of a draft. In fact, the original record, which in electronic systems is the first complete and effective record either received (if transmitted across space) or saved to a file in the system (if transmitted across time), ceases to exist after being stored for the first time. When recalled, the stored entity is a copy which, in the best of all possible scenarios, is a copy in the form of original, but, in most cases, is simply an imitative copy. Also a draft, while conceptually remaining the sketch or outline of the definitive document, prepared for purposes of correction and meant to be provisional, will only exist as an imitative or simple copy of the draft first stored. Thus, the official copy of each record will have to be subject to strict procedural controls that will serve as a form of authentication, considering that technologically based forms of authentication like the digital signature only serve when records are transmitted across space, as they usually constitute an obstacle to the maintenance of the record to which they are linked. Of course, when the official record is identified, so is the office of primary responsibility for that record, i.e. the office having the formal competence for maintaining the official records that share the same classification and retention period. This will also help to reduce duplication in the organization and designate accountability for the records.

Benchmark Requirement 8 — The eighth and last requirement prescribes that, if there is a transition of records from active status to semi-active and inactive status that involves the removal of records from the electronic system, the creator has established and implemented procedures determining what documentation has to be removed and transferred to the preserver along with the records. This documentation includes all the information necessary to access the records, to establish their identity, and to demonstrate their integrity. If the system generates record profiles, it will be sufficient to ensure that all records are accompanied by their profile. Otherwise, it may be necessary to transfer with the records audit trails, indexes, data directories, and data dictionaries, etc.

These eight requirements are intended to allow the preserver to assess, in the course of the process of appraisal, the authenticity of the electronic records of a creator before they are transferred to archival custody. They are cumulative, in the sense that the strength of the presumption of authenticity is based on the number of satisfied requirements and on the degree to which each individual requirement is satisfied. If the presumption of authenticity is weak, a verification of authenticity is necessary. The verification of authenticity is the act or process of establishing a correspondence between known facts about the record and the various contexts in which it has been created and maintained, and the proposed fact of the record's authenticity; it involves a detailed examination of the records in all their contexts and of reliable information available from other sources (e.g. audit trails, backups, copies preserved elsewhere, textual analysis, etc.).

Baseline requirements

After the records have been presumed or verified authentic and transferred to the custody of the preserver, their authenticity must be maintained by the preserver. To do so, the preserver must produce authentic copies of the records in question, because the production of authentic copies is the only way to ensure the preservation of electronic records. An electronic copy of an authentic electronic record is authentic if attested to be so by the official preserver, but such attestation must be supported by the preserver's ability to demonstrate that it has satisfied all the Baseline Requirements for the production of authentic copies. Only by virtue of this attestation is the copy deemed to conform to the record it reproduces until proof to the contrary is shown. For this reason, the second set of requirements, the Baseline Requirements, directed exclusively to the preserver, must all be implemented at the highest degree.

There are three Baseline Requirements.

Baseline Requirement 1 — The first requirement prescribes that the procedures and system(s) used

to transfer records to the archival institution or program, maintain them, and reproduce them embody adequate and effective controls to guarantee the records' identity and integrity, and specifically that:

- unbroken custody of the records is maintained
- security and control procedures are implemented and monitored
- the content of the record remains unchanged after reproduction

As part of the transfer process, the assessment of the authenticity of the records, which had occurred during the appraisal process, should be verified by ensuring that the attributes relating to the records' identity and integrity have been carried forward with the records themselves (Benchmark Requirement 1), along with any relevant documentation (Benchmark Requirement 8). Once the records have been transferred to archival custody, the preserver must establish many of the controls that were described in the Benchmark Requirements, i.e. the preserver must:

- establish access privileges concerning the access, use, and reproduction of the records within the archives, and ensure that they are implemented and monitored
- establish procedures to prevent, discover, and correct loss or corruption of records, as well as procedures to guarantee the continuing identity and integrity of the records against media deterioration and across technological changes
- establish rules determining responsibility for and means of authentication (if authentication is required)

Baseline Requirement 2 — The second requirement prescribes that the activity of reproduction be documented, and that this documentation includes:

- the date of the records' reproduction and the name of the responsible person
- the relationship between the records acquired from the creator and the copies produced by the preserver
- the impact of the reproduction process on their form, content, accessibility, and use
- the details of any copies of records known not to fully and faithfully reproduce the elements expressing the original identity and integrity

The documentation of the reproduction process is essential for the preserver to fulfil the role of trusted custodian of the record, for the user to have access to the history of reproduction (which becomes an integral part of the history of the record), and for future generations to be able to verify the authenticity of the records.

Baseline Requirement 3 — The third requirement prescribes that the archival description of the fonds containing the electronic records includes — in addition to information about the records' juridical-administrative, provenancial, procedural, and documentary contexts — information about changes the electronic records of the creator have undergone since they were first created. It has always been the function, either explicit or implicit, of archival description to authenticate the records and perpetuate their administrative and documentary relationships, but with electronic records this function has become indispensable. In fact, as original electronic records disappear and an interminable chain of non-identical reproductions follows them, in many cases the researchers looking at the last of those reproductions cannot find in them any information regarding provenance, authority, context, or authenticity. The authentication function of archival description is different from that of a certificate of authenticity, because it is a collective attestation of the authenticity of the records and of all their interrelationships as made explicit in the description rather than being simply an attestation of the authenticity of individual records. One might say that, given the mandatory documentation of each reproduction process carried out by the preserver, archival description is superfluous for the purposes of demonstrating the authenticity of the records copies themselves. However, if archival description summarizes the history of all reproductions, it obviates the need to preserve all the documentation of each reproduction and acts as a certificate of authenticity for the archival fonds.

Conclusion

The authenticity requirements have been tested on several aggregations of records and appear to work well in the context of database and document management systems. However, it has became apparent that technological developments are beginning to interfere with the procedures and forms of records creation, that decision-making is increasingly based on records whose creation and form are discretionary, and that great concern is developing about preserving and verifying the authenticity of new record types that are more and more common worldwide. For these reasons, a second phase of InterPARES has undertaken the development of an understanding of interactive and dynamic records resulting from artistic, scientific, and e-government activities, not only in the later phases of their life cycle but from the moment of their creation, in order to develop knowledge and strategies beneficial to both their creators and their preservers. This phase will be concluded by 2007.

Endnotes

1. Jenkinson, H. *A Manual of Archive Administration.* Oxford, UK: Clarendon Press, 1922, pp. 8–9, 39. Throughout this paper the terms archival document and record will be used interchangeably.

2. The InterPARES (International Research on Permanent Authentic Records in Electronic Systems) project was a collaborative, multidisciplinary, and international research endeavour that involved 60 researchers from 11 countries. Its aim was to develop the theoretical and methodological knowledge necessary for the long-term preservation of the authenticity of electronic records.

3. A record attribute is a defining characteristic of the record or of a record element. A record element is a constituent part of the record's documentary form. An attribute may manifest itself in one or more elements of a record's documentary form (e.g. the name of the author as superscription or as a signature) or in an annotation to the record (e.g. the archival bond as a record identifier) or in metadata in the audit trail, etc.

Résumé

Si les documents électroniques sont appelés à devenir aussi dignes de foi que les documents sur des supports traditionnels, les pratiques permettant de les créer, de les conserver et de les utiliser doivent être analysées, et des stratégies et des normes doivent être élaborées pour leur préservation authentique. C'est la mission qui a été confiée aux responsables d'un projet appelé InterPARES (International research on Permanent Authentic Records in Electronic Systems [recherche internationale sur les documents authentiques permanents dans les systèmes électroniques]) qui ont énoncé deux séries d'exigences en matière d'authenticité pour les documents administratifs générés ou conservés dans des bases de données ou des systèmes de gestion de documents : les exigences-repères à l'appui de la présomption de l'authenticité des documents électroniques, et les exigences de base en vue de la production de copies authentiques de documents électroniques. Une deuxième phase du projet InterPARES a été lancée avec l'étude de l'applicabilité de ces exigences à des documents interactifs, dynamiques et expérientiels produits dans le cadre d'activités artistiques, scientifiques et cybergouvernementales. La communication portera sur les exigences en matière d'authenticité et examinera le défi que pose, pour leur application, la complexité de nouveaux types de documents numériques.