Appendix 2

Requirements for Assessing and Maintaining the Authenticity of Electronic Records

Authenticity Task Force

March 2002

The requirements that are identified in this document fall into two groups: requirements that support the presumption of the authenticity of electronic records before they are transferred to the custody of the preserver,[1] and requirements that support the production of authentic copies of electronic records that have been transferred to the custody of the preserver. The report is organized into the following sections:

- Conceptual Framework for the Requirements for Assessing and Maintaining the Authenticity of Electronic Records
- Benchmark Requirements Supporting the Presumption of Authenticity of Electronic Records
- Baseline Requirements Supporting the Production of Authentic Copies of Electronic Records
- Commentary on the Benchmark Requirements Supporting the Presumption of Authenticity of Electronic Records
- Commentary on the Baseline Requirements Supporting the Production of Authentic Copies of Electronic Records

Conceptual Framework for the Requirements for Assessing and Maintaining the Authenticity of Electronic Records

Introduction

Authenticity is defined as "the quality of being authentic, or entitled to acceptance."[2] *Authentic* means "worthy of acceptance or belief as conforming to or based on fact" and is synonymous with the terms *genuine* and *bona fide*. *Genuine* "implies actual character not counterfeited, imitated, or adulterated [and] connotes definite origin from a source." *Bona fide* "implies good faith and sincerity of intention".[3] From these definitions it follows that an *authentic record* is a record that is what it purports to be and is free from tampering or corruption.

In both archival theory and jurisprudence, records that the creator[4] relies on in the usual and ordinary course of business are presumed authentic. However, digital information technology creates significant risks that electronic records may be altered, either inadvertently or intentionally. Therefore, in the case of records maintained in electronic systems, the presumption of authenticity must be supported by evidence that a record is what it purports to be and has not been modified or corrupted in essential respects. To assess the authenticity of an electronic record, the preserver must be able to establish its *identity* and demonstrate its *integrity*.

The identity of a record refers to the distinguishing character of a record, that is, the attributes of a record that uniquely characterize it and distinguish it from other records. From an archival-diplomatic perspective, such attributes include: the names of the persons concurring in its formation (i.e., its author, addressee, writer, and originator); its date(s) of creation (i.e., the date it was made, received, and set aside) and its date(s) of transmission; an indication of the action or matter in which it participates; the expression of its archival bond, which links it to other records participating in the same action (e.g., a classification code or other unique identifier); as well as an indication of any attachment(s) since an attachment is considered an

---

[1] The preserver is the juridical person whose primary responsibility is the long-term preservation of authentic records. The preserver's responsibilities include appraisal.

[2] *Oxford English Dictionary*, 2nd ed., s.v. "authenticity."

[3] *Merriam-Webster Online Collegiate Dictionary*, s.v. "authentic."

[4] The creator is the physical or juridical person in whose archival fonds the record exists. The fonds is the whole of the records created (meaning made or received and set aside for action or reference) by a physical or juridical person in the course of carrying out its activities.

integral part of a record.[5] The attributes[6] that establish the identity of a record may be explicitly expressed in an element of the record, in metadata related to the record, or they may be implicit in its various contexts. Those contexts include: its *documentary context*, that is, the archival fonds to which a record belongs, and its internal structure; its *procedural context*, that is, the business process in the course of which the record is created; its *technological context*, that is, the characteristics of the technical components of an electronic computing system in which records are created; its *provenancial context*, that is, the creating body, its mandate, structure, and functions; and its *juridical-administrative* context, that is, the legal and organizational system in which the creating body belongs.

The *integrity* of a record refers to its wholeness and soundness: a record has integrity when it is complete and uncorrupted in all its essential respects. This does not mean that the record must be precisely the same as it was when first created for its integrity to exist and be demonstrated. Even in the paper world, with the passage of time, records are subject to deterioration, alteration and/or loss. In the electronic world, the fragility of the media, the obsolescence of technology, and the idiosyncrasies of systems likewise affect the integrity of records. When we refer to an electronic record, we consider it essentially complete and uncorrupted if the message that it is meant to communicate in order to achieve its purpose is unaltered. This implies that its physical integrity, such as the proper number of bit strings, may be compromised, provided that the articulation of the content and any required annotations and elements of documentary form remain the same.[7] The integrity of a record may be demonstrated by evidence found on the face of the record, in metadata related to the record, or in one or more of its various contexts.

Assessing the Authenticity of Electronic Records

The records of the creator belong to one of two categories. The first category comprises those records that exist as created. They are considered authentic because they are the same as they were in their first instantiation. The second category comprises those records that have undergone some change and therefore cannot be said to exist as first created; they are considered authentic because the creator treats them as such by relying on them for action or reference in the regular conduct of business. However, the authenticity of electronic records is threatened whenever they are transmitted across space (i.e., when sent to an addressee or between systems or applications) or time (i.e., either when they are in storage, or when the hardware or software used to store, process, or communicate them is updated or replaced). Given that the acts of setting aside an electronic record for future action or reference and of retrieving it inevitably entail moving it across significant technological boundaries (from display to storage subsystems and vice versa), virtually all electronic records belong to the second category. Therefore, the preserver's inference of the authenticity of electronic records must be further supported by evidence—provided in association with the records—that they have been maintained using technologies and administrative procedures that either guarantee their continuing identity and integrity or at least minimize risks of change from the time the

---

[5] An attachment is a document that constitutes an integral part of the whole record, notwithstanding the fact that it exists as a linked, but physically separate entity.

[6] The use of the terms *attribute* and *element* in this report should not be confused with the way the terms are used in other contexts, such as the various Standard Generalized Mark-up Languages (SGML). In this report, a record attribute is a defining characteristic of a record or of a record element. A *record element* is a constituent part of the record's documentary form and may be either extrinsic or intrinsic. An attribute may manifest itself in one or more elements of a record's documentary form. For example, the name of the author of a record is an attribute, which may be expressed as a superscription or a signature, both of which are intrinsic elements of documentary form. For a more detailed explanation of the extrinsic and intrinsic elements of documentary form see the Authenticity Task Force's *Template for Analysis,* in Appendix 1. An attribute may also manifest itself in the form of an annotation(s) to a record, in metadata linked to it, or in one or more of its various contexts.

[7] For example, for an electronic mail message, an authentic copy of a complete message may include only the text. Provided it clearly indicated the author, addressee, receivers, and date as well as the content, it would not need to appear in the same way in which it was seen by the author or addressee. In contrast, an authentic copy of a map would have to retain its original presentation features, including colour and feature presentation. Provided these requirements were met, an authentic copy could be produced in GIF, JPEG, or GML format.

records were first set aside to the point at which they are subsequently accessed. The requirements for assessing the authenticity of the creator's electronic records concern this evidence.

The Presumption of Authenticity

A presumption of authenticity is an inference that is drawn from known facts about the manner in which a record has been created and maintained. The evidence that supports the presumption that the record creator created and maintained them authentic are enumerated in the Benchmark Requirements Supporting the Presumption of Authenticity of Electronic Records (Requirement Set A). A presumption of authenticity will be based upon the number of requirements that have been met and the degree to which each has been met. The requirements are, therefore, cumulative: the higher the number of satisfied requirements, and the greater the degree to which an individual requirement has been satisfied, the stronger the presumption of authenticity. This is why these requirements are termed "benchmark" requirements.

The Verification of Authenticity

In any given case, there may be an insufficient basis for a presumption of authenticity, or the presumption may be extremely weak. In such cases, further analysis may be necessary to verify the authenticity of the records. A 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.[8] In the verification process, the known facts about the record and its contexts provide the grounds for supporting or refuting the contention that the record is authentic. Unlike the presumption of authenticity, which is established on the basis of the benchmark requirements, this verification involves a detailed examination of the records themselves and reliable information available from other sources about the records and the various contexts in which they have been created and maintained. Methods of verification include, but are not limited to, a comparison of the records in question with copies that have been preserved elsewhere or with back-up tapes; comparison of the records in question with entries in a register of incoming and outgoing records; textual analysis of the record's content; forensic analysis of the medium, script, and so on; a study of audit trails; and the testimony of a trusted third party.

Maintaining the Authenticity of Electronic Records

After the records have been presumed or verified authentic in the appraisal process, and have been transferred from the creator to the preserver, their authenticity needs to be maintained by the preserver. In order to do so, the preserver must carry forward the records in accordance with the baseline requirements that apply to the maintenance of records, producing copies according to procedures that also maintain authenticity.[9] The production of authentic copies is regulated by the Baseline Requirements Supporting the Production of Authentic Copies of Electronic Records (Requirement Set B). Unlike the benchmark requirements, all of the requirements included in the baseline requirements must be met before the preserver can attest to the authenticity of the electronic copies in its custody. This is why the requirements for the production of authentic electronic copies are termed "baseline" requirements.

Satisfaction of these baseline requirements will enable the preserver to certify that copies of electronic records are authentic. Traditionally, the official preserver of the records has been the person entrusted with issuing authentic copies of such records. To fulfill that role, the preserver needed simply to attest that the

---

8 In common usage, *verify* is synonymous with the terms validate, confirm, corroborate, and *substantiate*. According to *Merriam-Webster Online Collegiate Dictionary, "validate* means to attest to the truth or validity of something; *confirm* implies the removing of doubts by an authoritative affirmation or by factual proof; *corroborate* suggests the strengthening of something that is already partly established; substantiate implies the offering of evidence that sustains the contention."

9 It is understood that the records maintained by the preserver exist only as copies of the creator's records.

copy conformed to the record being reproduced. With electronic records, and the accompanying difficulties related to preservation, the prudent path would be for the preserver to produce and maintain documentation relating to the manner in which it has maintained the records over time as well as the manner in which it has reproduced them to support its attestation of authenticity.

A copy is the result of a reproduction process. A copy can be made from an original or from a copy of either an original or another copy.[10] There are several types of copy. The most reliable copy is a copy in the form of an original, which is identical to the original although generated subsequently. An imitative copy is a copy that reproduces both the content and form of the record, but in such a way that it is always possible to tell the copy from the original. A simple copy is a copy that reproduces only the content of the original.

Any of these types of copy is authentic if attested to be so by the official preserver. By virtue of this attestation, the copy is deemed to conform to the record it reproduces until proof to the contrary is shown. Such attestation is supported by the preserver's ability to demonstrate that it has satisfied the applicable baseline requirements for maintenance and all of the requirements for the production of authentic copies.

Benchmark Requirements Supporting the Presumption of Authenticity of Electronic Records

Preamble

The benchmark requirements are the conditions that serve as a basis for the preserver's assessment of the authenticity of the creator's electronic records. Satisfaction of these benchmark requirements will enable the preserver to infer a record's authenticity on the basis of the manner in which the records have been created, handled, and maintained by the creator.

Within the benchmark requirements, Requirement A.1 identifies the core information about an electronic record—the immediate context of its creation and the manner in which it has been handled and maintained—that establishes the record's identity and lays a foundation for demonstrating its integrity. Requirements A.2–A.8 identify the kinds of procedural controls over the record's creation, handling, and maintenance that support a presumption of its integrity.

[10] In common language, *copy* and *reproduction* are synonyms. For the purposes of this research, the term *reproduction* is used to refer to the process of generating a copy, while the term *copy* is used to refer to the result of such a process, that is, to any entity which resembles and is generated from the records of the creator. An original record is the first, complete record, which is capable of achieving its purposes (i.e., it is effective). A record may also take the form of a draft, which is a temporary compilation made for purposes of correction.

Benchmark Requirements (Requirement Set A)

To support a presumption of authenticity the preserver must obtain evidence that:

REQUIREMENT A.1: Expression of Record Attributes and Linkage to Record	the value of the following attributes 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, that is:

- name of author[11]
- name of writer [12](if different from the author)
- name of originator[13] (if different from name of author or writer)
- name of addressee[14]

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

A.1.a.iii Date(s) of creation and transmission, that is:

- chronological date[15]
- received date[16]
- archival date[17]
- transmission date(s)[18]

A.1.a.iv Expression of archival bond[19] (e.g., classification code, file identifier)

[11] The name of the physical or juridical person having the authority and capacity to issue the record or in whose name or by whose command the record has been issued.

[12] The name of the physical or juridical person having the authority and capacity to articulate the content of the record.

[13] The name of the physical or juridical person assigned the electronic address in which the record has been generated and/or sent.

[14] The name of the physical or juridical person(s) to whom the record is directed or for whom the record is intended.

[15] The date, and possibly the time, of compilation of a record included in the record by the author or the electronic system on the author's behalf.

[16] The date, and possibly the time, when a record is received by the addressee.

[17] The date, and possibly the time, when a record is officially incorporated into the creator's records.

[18] The date and time when a record leaves the space in which it was generated.

[19] The archival bond is the relationship that links each record, incrementally, to the previous and subsequent ones and to all those participate in the same activity. It is originary (i.e., it comes into existence when a record is made or received and set aside), necessary (i.e., it exists for every record), and determined (i.e., it is characterized by the purpose of the record).

A.1.a.v Indication of attachments

A.1.b Integrity of the record:

A.1.b.i Name of handling office[20]

A.1.b.ii Name of office of primary responsibility[21] (if different from handling office)

A.1.b.iii Indication of types of annotations added to the record[22]

A.1.b.iv Indication of technical modifications;[23]

REQUIREMENT A.2: Access Privileges	the creator has defined and effectively implemented access privileges concerning the creation, modification, annotation, relocation, and destruction of records;

REQUIREMENT A.3: Protective Procedures: Loss and Corruption of Records	the creator has established and effectively implemented procedures to prevent, discover, and correct loss or corruption of records;

REQUIREMENT A.4: Protective Procedures: Media and Technology	the creator has established and effectively implemented procedures to guarantee the continuing identity and integrity of records against media deterioration and across technological change;

REQUIREMENT A.5: Establishment of Documentary Forms	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;

[20] The office (or officer) formally competent for carrying out the action to which the record relates or for the matter to which the record pertains.

[21] The office (or officer) given the formal competence for maintaining the authoritative record, that is, the record considered by the creator to be its official record.

[22] Annotations are additions made to a record after it has been completed. Therefore, they are not considered elements of the record's documentary form.

[23] Technical modifications are any changes in the digital components of the record as defined by the Preservation Task Force. Such modifications would include any changes in the way any elements of the record are digitally encoded and changes in the methods (software) applied to reproduce the record from the stored digital components; that is, any changes that might raise questions as to whether the reproduced record is the same as it would have been before the technical modification. The indication of modifications might refer to additional documentation external to the record that explains in more detail the nature of those modifications.

REQUIREMENT A.6: Authentication of Records	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 the means of authentication;

REQUIREMENT A.7: Identification of Authoritative Record	if multiple copies of the same record exist, the creator has established procedures that identify which record is authoritative;

REQUIREMENT A.8: Removal and Transfer of Relevant Documentation	if there is a transition of records from active status to semi-active and inactive status, which involves the removal of records from the electronic system, the creator has established and effectively implemented procedures determining what documentation has to be removed and transferred to the preserver along with the records.

Baseline Requirements Supporting the Production of Authentic Copies of Electronic Records

Preamble

The baseline requirements outline the minimum conditions necessary to enable the preserver to attest to the authenticity of copies of inactive electronic records.

Baseline Requirements (Requirement Set B)

The preserver should be able to demonstrate that:

REQUIREMENT B.1: Controls over Records Transfer, Maintenance, and Reproduction	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 **B.1.a** Unbroken custody of the records is maintained; **B.1.b** Security and control procedures are implemented and monitored; and **B.1.c** The content of the record and any required annotations and elements of documentary form remain unchanged after reproduction.

REQUIREMENT B.2: Documentation of Reproduction Process and its Effects	the activity of reproduction has been documented, and this documentation includes ***B.2.a*** The date of the records' reproduction and the name of the responsible person;

	B.2.b The relationship between the records acquired from the creator and the copies produced by the preserver; **B.2.c** The impact of the reproduction process on their form, content, accessibility and use; and **B.2.d** In those cases where a copy of a record is known not to fully and faithfully reproduce the elements expressing its identity and integrity, such information has been documented by the preserver, and this documentation is readily accessible to the user;

REQUIREMENT B.3: Archival Description	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.

Commentary on the Benchmark Requirements Supporting the Presumption of Authenticity of Electronic Records

The assessment of the authenticity of the creator's records takes place as part of the appraisal process. That process and the role of the benchmark requirements within it are described in more detail in the "Appraisal Task Force Report." This assessment should be verified when the records are transferred to the preserver's custody.

A.1: Expression of Record Attributes and Linkage to Record

The presumption of a record's authenticity is strengthened by knowledge of certain basic facts about it. The attributes identified in this requirement embody those facts. The requirement that the attributes be expressed explicitly and linked inextricably[24] to the record during its life, and carried forward with it over time and space, reflects the task force's belief that such expression and linkage provide a strong foundation on which to establish a record's identity and demonstrate its integrity. The case studies undertaken as part of the work of the task force revealed very little consistency in the way the attributes that specifically establish the identity of a record are captured and expressed from one electronic system to another. In certain systems, some attributes were explicitly mentioned on the face of the record; in others they could be found in a wide range of metadata linked to the record or they were simply implicit in one or more of the record's contexts. In many cases, certain attributes (e.g., the expression of the archival bond) were not captured at all. The task force's concern is that, in the absence of a precise and explicit statement of the basic facts concerning a record's identity and integrity, it will be necessary for the preserver to acquire enormous, and otherwise unnecessary, quantities of data and documentation simply to establish those facts.

The link between the record and the attributes listed in Requirement A.1 is viewed by the task force as a *conceptual* rather than a *physical* one, and the requirement could be satisfied in different ways, depending on the nature of the electronic system in which the record resides. For example, in electronic records management systems, this requirement is usually met through the creation of a record profile.[25] In other types of systems, the requirement could be fulfilled through a topic map. A topic map expresses the characteristics (i.e., *topics*) of subjects (e.g., records or record attributes) and the relationships between and among them.

When a record is exported from the live system, migrated in a system update, or transferred to the preserver, the attributes should be linked to the record and available to the user. When pulling together the

[24] For the purposes of this requirement, inextricable means incapable of being disentangled or untied, and link means a connecting structure.

[25] If the attribute values contained in the profile are also expressed independently as entries in a register of all records made or received by the creator, then, in addition to establishing the identity and supporting the inference of the integrity of the record, they would corroborate such identity and strengthen the inference of integrity.

data prior to export, the creator should also ensure that the data captured are the right data. For example, in the case of distribution lists, the creator must ensure that if the recipients specified on "List A" were changed at some point in the active life of records, the accurate "List A: Version 1" is exported with the records associated with the first version, and that the second version is sent forward with those records sent to recipients on "List A: Version 2."

A.2 Access Privileges

Defining access privileges means assigning responsibility for the creation, modification, annotation, relocation, and destruction of records on the basis of competence, which is the authority and capacity to carry out an administrative action. Implementing access privileges means conferring exclusive capability to exercise such responsibility. In electronic systems, access privileges are usually articulated in tables of user profiles. Effective implementation of access privileges involves the monitoring of access through an audit trail that records every interaction that an officer has with each record (with the possible exception of viewing the record). If the access privileges are not embedded within the electronic system but are based on an external security system (such as the exclusive assignment of keys to a location), the effective implementation of access privileges will involve monitoring the security system.

A.3 Protective Procedures: Loss and Corruption of Records

Procedures to protect records against loss or corruption include: prescribing regular back-up copies of records and their attributes; maintaining a system back-up that includes system programs, operating system files, etc.; maintaining an audit trail of additions and changes to records since the last periodic back-up; ensuring that, following any system failure, the back-up and recovery procedures will automatically guarantee that all complete updates (records and any control information such as indexes required to access the records) contained in the audit trail are reflected in the rebuilt files and also guarantee that any incomplete operation is backed up. The capability should be provided to rebuild forward from any back-up copy, using the back-up copy and all subsequent audit trails.

A.4 Protective Procedures: Media and Technology

Procedures to counteract media fragility and technological obsolescence include: planning upgrades to the organization's technology base; ensuring the ability to retrieve, access, and use stored records when components of the electronic system are changed; refreshing the records by regularly moving them from one storage medium to another; and migrating records from an obsolescent technology to a new technology.

A.5 Establishment of Documentary Forms

The documentary form of a record may be determined in connection to a specific administrative procedure, or in connection to a specific phase(s) within a procedure. The documentary form may be prescribed by business process and work-flow control technology, where each step in an administrative procedure is identified by specific record forms. If a creator customizes a specific application, such as an electronic mail application, to carry certain fields, the customized form becomes, by default, the required documentary form. It is understood that the creator, acting either on the basis of its own needs or the requirements of the juridical system, not an individual officer, establishes the required documentary form(s) of records.

When the creator establishes the documentary form in connection to a procedure, or to specific phases of a procedure, it is understood that this includes the determination of the intrinsic and extrinsic elements of form[26] that will allow for the maintenance of the authenticity of the record. Because, generally speaking, that determination will vary from one form of a record to another, and from one creator to another, it is not possible to predetermine or generalize the relevance of specific intrinsic and extrinsic elements of documentary form in relation to authenticity.

A.6 Authentication of Records

In common usage, to authenticate means to prove or serve to prove the authenticity of something. More specifically, the term implies establishing genuineness by adducing legal or official documents or expert opinion. For the purposes of the benchmark requirements, authentication is understood to be a declaration of a record's authenticity at a specific point in time by a juridical person entrusted with the authority to make such declaration. It takes the form of an authoritative statement (which may be in the form of words or

[26] The extrinsic and intrinsic elements of form are defined and explained in the Authenticity Task Force's *Template for Analysis,* Appendix 1.

symbols) that is added to or inserted in the record attesting that the record is authentic.[27] The requirement may be met by linking the authentication of specific types of records to business procedures and assigning responsibility to a specific office or officer for authentication.

The authentication of copies differs from the validation of the process of reproduction of the digital components of the records. The latter process occurs every time the records of the creator are moved from one medium to another or migrated from one technology to another.

A.7 Identification of Authoritative Record

An authoritative record is a record that is considered by the creator to be its official record and is usually subject to procedural controls that are not required for other copies. The identification of authoritative records corresponds to the designation of an office of primary responsibility as one of the components of a record retention schedule. The Office of Primary Responsibility is the office given the formal competence for maintaining the authoritative (that is, official) records belonging to a given class within an integrated classification scheme and retention schedule. The purpose of designating an Office of Primary Responsibility for each class of record is to reduce duplication and to designate accountability for records.

It is understood that in certain circumstances there may be multiple authoritative copies of records, depending on the purpose for which the record is created.

A.8 Removal and Transfer of Relevant Documentation

This requirement implies that the creator needs to carry forward with the removed records all the information that is necessary to establish the identity and demonstrate the integrity of those records, as well as the information necessary to place the records in their relevant contexts.

Commentary on the Baseline Requirements Supporting the Production of Authentic Copies of Electronic Records

The establishment and implementation of the baseline requirements take place as part of the function of managing preservation. The preservation function and the role of the baseline requirements within it are described in more detail in the "Preservation Task Force Report."

B.1 Controls over Records Transfer, Maintenance, and Reproduction

The controls over the transfer of electronic records to archival custody include establishing, implementing, and monitoring procedures for registering the records' transfer; verifying the authority for transfer; examining the records to determine whether they correspond to the records that are designated in the terms and conditions governing their transfer; and accessioning the records.

As part of the transfer process, the assessment of the authenticity of the creator's records, which has taken place as part of the appraisal process, should be verified. This includes verifying that the attributes relating to the records' identity and integrity have been carried forward with them (Requirement A.1), along with any relevant documentation (Requirement A.8).

The controls over the maintenance of electronic records once they have been transferred to archival custody are similar to several of the ones enumerated in the benchmark requirements. For example, the preserver should establish access privileges concerning the access, use, and reproduction of records (Requirement A.2); establish procedures to prevent, discover, and correct loss or corruption of records (Requirement A.3), as well as procedures to guarantee the continuing identity and integrity of records against media deterioration and across technological change (Requirement A.4). Once established, the privileges and procedures should be effectively implemented and regularly monitored. If authentication of the records is

[27] The meaning of authentication as it is used by the Authenticity Task Force in this report is broader than its meaning in public key infrastructure (PKI) applications. In such applications, authentication is restricted to proving identity and public key ownership over a communication network.

required, the preserver should establish specific rules regarding who is authorized to authenticate them and the means of authentication that will be used (Requirement A.6).

The controls over the reproduction of records include establishing, implementing, and monitoring reproduction procedures that are capable of ensuring that the content of the record is not changed in the course of reproduction.

B.2 Documentation of Reproduction Process and its Effects

Documenting the reproduction process and its effects is an essential means of demonstrating that the reproduction process is transparent (i.e., free from pretence or deceit). Such transparency is necessary to the effective fulfilment of the preserver's role as a trusted custodian of the records. Documenting the reproduction process and its effects is also important for the users of records since the history of reproduction is an essential part of the history of the record itself. Documentation of the process and its effects provides users of the records with a critical tool for assessing and interpreting the records.

B.3 Archival Description

Traditionally it has been a function of archival description to authenticate the records and perpetuate their administrative and documentary relationships. With electronic records, this function becomes critical. Once the records no longer exist except as authentic copies, the archival description is the primary source of information about the history of the record, that is, its various reproductions and the changes to the record that have resulted from them. While it is true that the documentation of each reproduction of the record copies[28] may be preserved, the archival description summarizes the history of all the reproductions, thereby obviating the need to preserve all the documentation for each and every reproduction. In this respect, the description constitutes a collective attestation of the authenticity of the records and their relationships in the context of the fonds to which the records belong. This is different from a certificate of authenticity, which attests to the authenticity of individual records. The importance of this collective attestation is that it authenticates and perpetuates the relationships between and among records within the same fonds.

[28] Although, technically, every reproduction of a record that follows its acquisition by the preserver is an authentic copy, it is the only record that exists and, therefore, should normally be referred to as "the record" rather than as "the copy."