Managing Authenticity through the Digital Resource Lifecycle*

Maria Guercio and Silvio Salza

Università degli studi di Roma "La Sapienza"
maria.guercio@uniroma1.it,
salza@dis.uniroma1.it

Abstract. On the basis of principles and methodologies developed by the major projects on digital preservation, the paper addresses the fundamental problem of authenticity management, and specifically of defining appropriate mechanisms and tools to transform the presumption of authenticity into the capacity of its verification. The approach we propose is to concentrate on the digital resource lifecycle, since, in order to make a proper assessment, one must be able to trace back all the transformations the digital resource has undergone since its creation, and that may have affected its authenticity. For these transformations one needs to collect and preserve the appropriate evidence that would allow, at a later time, to make the assessment. We have therefore developed a model of the digital resource lifecycle in order to identify the main events that impact on authenticity and to define precise operational guidelines to specify which evidence should be collected and how to organize it. A case study analysis is currently being performed to check the validity of the model and to see how it specializes on several specific environments. Preliminary results are already available and confirm that the model is sound and that the implementation of the guidelines can be worked out effectively and with a fairly reasonable amount of effort.

Keywords: authenticity, curation, long-term preservation, repository.

1 Introduction

Authenticity is considered in the literature and by all major projects on digital preservation in the area of digital libraries and institutional repositories as one of the most crucial characteristics to be maintained over time and consistently documented for evidence and future use [1-4]. In the last decade the scientific community has developed robust principles and a basic methodological approach to this issue, with the aim of establishing among different communities a common understanding of the concepts involved and on the specific tools to be implemented.

The InterPARES projects (1999-2012) [5] have addressed the creation, maintenance and preservation of digital records, with specific reference to authenticity. A

* Work partially supported by European Community under the Information Society Technologies (IST) program of the 7th FP for RTD - project APARSEN, ref. 269977.

M. Agosti et al. (Eds.): IRCDL 2012, CCIS 354, pp. 249–260, 2013.

major finding is that, to preserve *trustworthy digital records* (i.e., records that can be demonstrated to be *reliable*, *accurate* and *authentic*), records creators must create them in such a way and in such a form that it is possible to maintain and preserve them. This entails that a relationship between a records creator and its designated preserver must begin at the time the records are created.

The CASPAR project (2006-2009) [6] has dedicated specific effort in developing a methodology for the management of authenticity in the digital environment. In particular the Caspar Authenticity Team has identified a set of attributes that allow to capture information relevant for the authenticity as it can be collected along the lifecycle of the digital resources; the Team has also developed tools and procedures to manage this information.

On the basis of this analysis, a well stated terminology has been included in the new version of the OAIS reference model [1] [8], and considerable agreement has been reached in the digital preservation community on some basic principles:

- it is not possible (feasible) to preserve electronic resources as *original unchanged resources*: one may have only the ability to reproduce them in the form of *authentic copies* thanks to the preservation of authentic copies of digital components;
- authenticity *cannot be recognized as given once and for ever* within a digital environment: a clear distinction should be made between the authenticity of the preserved record/resource (not necessarily the same objects as those originally deposited) and the procedure of *evaluating* and *validating* the same object;
- the profile of the authenticity has to be considered as a *process* aimed at gathering, protecting and/or evaluating information/set of attributes mainly about identity and integrity of the digital resource.

As a consequence of this, and because digital resources curation is increasingly and dynamically based on the concept of *trust* [2], the heart of the problem has become how to support the unavoidable principle of trustworthiness and, even more, how to transform these general concepts and assumptions into a series of concrete, measurable and well interconnected steps to sustain the presumption of digital authenticity both in the pre-ingest phase and in the repository itself.

In other words, the fundamental question is how to transform *presumption* into *evidence,* and how to define a multilayer approach able to provide a convincing structured series of events, agents and information, related to the interconnected phases of the digital resources lifecycle, in order to verify their integrity and authenticity conveniently to the various levels of analysis and according to the specific needs of consumers.

---

[1] In the draft of the new standard authenticity is defined as: "the degree to which a person (or system) may regard an object as what it is purported to be. The degree of authenticity is judged on the basis of evidence".

[2] In the Merriam-Webster dictionary trust is identified as "a charge or duty imposed in faith or confidence or as a condition of some relationship", a sort of "glue which binds that relationship together", whose ingredients have to be identified and described for effectiveness of the custody.

These questions have been thoroughly addressed by the APARSEN project [9], a NOE funded by the EU (2011-2014) with the goal of overcoming the fragmentation of the research and of the development in the digital preservation area by bringing together major European players, to combine and integrate these efforts into a shared program of work, thereby creating a pre-eminent virtual research centre in digital preservation in Europe.

The activity carried on in APARSEN has concentrated on establishing operational guidelines to properly manage the digital resource lifecycle in order to:

- conveniently trace (for future verification) all the transformations the digital resource has undergone since its creation that may have affected its authenticity and provenance,
- collect and preserve for each of these transformations the appropriate evidence that would allow, at a later time, to make the assessment and, more precisely,
- develop a model of the digital resource lifecycle, which identifies the main events that impact on authenticity and provenance and investigate in detail, for each of them the evidence that has to be gathered in order to conveniently document the history of the digital resource.

The final target of this effort is, of course, trying to achieve the interoperability among the systems where the digital resource is kept or preserved along its lifecycle, since there may be several changes of custody, and therefore very often the evidence about authenticity needs to be managed and interpreted by systems that are different from the ones that gathered it.

Indeed the model we present in this paper is based on a broad analysis of the main standards developed or supported by the major research projects in the preservation area [12-16]. Because the focus is set on the events and the responsibilities in the various phases of lifecycle (creation, keeping, preservation), the main standards that have been considered are (apart from OAIS [7], which is the basis of our common understanding in building an open framework for digital preservation) those concerning the creation and keeping of accurate, complete and reliable records in the e-government field. Even if intended for a specific domain, these rules are relevant for the preservation of any type of resources.

Achieving such an ambitious goal requires time, consensus and a thorough discussion. For this reason the methodology we propose in the following sections, although we already have some encouraging feedback from test applications, should only be considered as a preliminary step, and a basis to derive more complete operational guidelines to improve the current (too often very poor) practices in managing digital authenticity and providing evidence in preservation systems.

2 Authenticity and the Digital Resource Lifecycle

In order to properly assess the authenticity of a Digital Resource (DR) we must be able to trace back, along the whole extent of its lifecycle since its creation, all the transformations the DR has undergone and that may have affected its authenticity and

provenance. For each of these transformations [10] one needs then to collect and preserve the appropriate evidence that would allow, at a later time, to make the assessment, and that we shall call therefore *authenticity evidence*.

Under quite general assumptions, we may consider the DR lifecycle as divided in three phases:

- **Pre-ingest.** This phase begins when the DR is delivered for the first time to a keeping system and goes on until the DR is submitted to a *Long Time Digital Preservation (LTDP) system*. During the pre-ingest phase, the DR may be transferred between several keeping systems and may undergo several transformations.
- **Ingestion.** This phase encompasses both the transfer of the DR from the producer to the LTDP system, and the subsequent control and transformations the DR undergoes during the ingest, which, referring to the OAIS terminology, marks the passage between the SIP (Submission Information Package) and the AIP (Archival Information Package).
- **Long term preservation.** This phase begins after the DR is ingested by a LTDP system and goes on as long as the DR is preserved. As for the pre-ingest and the ingest phases, also during the LTDP phase the DR may undergo several transformations, notably format migrations, aggregations etc. Moreover it may get moved from a LTDP system to another one.

The pre-ingest phase has been introduced as a separate phase from the ingest to represent the part of the lifecycle that occurs before the delivery to the DR of a LTDP system. Collecting evidence for all the transformations the DR undergoes during this phase is of the utmost importance to assess the its authenticity.

Each transformation a DR undergoes during its lifecycle is connected to an *event*, which occurs under the responsibility of one or more people, whom we shall call *agents*. A transformation may involve one or several DRs and one or several agents, and produces as a result a set of DRs, possibly new versions of the ones that were the object of the transformations.

A very ambitious goal would be to try to determine 'all' possible events that are relevant with regard to the authenticity of a DR, and to draw precise guidelines to specify which authenticity evidence should be collected for each of these events, and how to organize it.

This would be indeed a very interesting result since, as we have seen, the DR moves along its lifecycle from system to system, and therefore these systems, when they exchange the DR, need to interoperate in order to exchange also the related authenticity evidence. Interoperability means agreeing on a common ground, and therefore common guidelines would form the basis that would allow such systems to interoperate.

3 The Core Set of Lifecycle Events

Unfortunately, the variety of events that may occur during the DR lifecycle is very large and depends, at least in part, from the specific environment. Nevertheless, it is

possible to consider at least a minimal *core set of events*, that includes the most important ones, as well as the ones which are likely to occur in most of the environments in which DRs are produced and managed. The core set should be considered as a sort of common basis on which different keeping and preservation systems may agree, thus achieving at least a basic degree of interoperability in the exchange and management of authenticity evidence.

In our investigation we have considered a reasonable variety of environments, notably natural science data, health care data, social science data and administrative data repositories. As a result of our analysis, we have proposed the core set of events that we briefly outline in the following subsections. For a more complete description one should refer directly to the APARSEN project documentation [10].

3.1 Pre-ingest Phase

The author of a DR is the person who, individually or as the representative of an institution, takes the responsibility of the content of the DR and of the descriptive information associated to it, when the DR is created in the pre-ingest phase i.e. delivered for the first time to a keeping system, a term by which we mean any kind of system where the DR is kept, once it has been created, until it is submitted to a LTDP system.

This definition encompasses a large variety of situations. For instance in a scientific experimental environment, where a DR is a collection of experimental data, the author is the scientist in charge of the experimental measures, who certifies the authenticity and the integrity of the data and of the associated descriptive information, and the keeping system is the computer system used to store and managed the experimental data, for instance a data base centered system. Similarly, in a document management environment, where the DR is an electronic document, the author is the person who prepares the final version of the document, and the keeping system is the Electronic Record Management System (ERMS) where the document is kept.

During its stay in the keeping system the DR may undergo a series of transformations that may affect both its content of the DR and the descriptive information associated to it. For instance the DR may go through format migrations (even before it enters the LTDP custody), or it may get integrations of its content and/or of its metadata, or it may eventually be aggregated with other DRs to form a new DR. Moreover, before getting to LTDP, the DR may be transferred, one or several times, between different keeping systems.

In the model, the core set for the pre-ingest phase comprises the following events:

- **CAPTURE:** the DR is delivered by its author to a keeping system;
- **INTEGRATE:** new information is added to a DR already stored in the keeping system;
- **AGGREGATE:** several DR, already stored in the keeping system, are aggregated to form a new DR;
- **DELETE:** a DR, stored in the keeping system is deleted, after its preservation time has expired, according to a stated policy;
- **MIGRATE:** one or several components of the DR are converted to a new format;
- **TRANSFER:** a DR is transferred between two keeping systems.

3.2 Ingest Phase

In the model, the ingest phase includes also the submission of the DR to the preservation repository. It involves therefore both the system where the DR was kept and the LTDP system to which is delivered.

The content and the structure of the SIP (Submission Information Package) through which the DR is delivered must comply with a submission agreement established between the system where the DR was kept (i.e. the Producer in the OAIS reference model) and the LTDP system (the OAIS). After the submission, the DR may eventually be deleted in the origin system, but this action should be considered a separate event. The DR identity is maintained in the keeping system, but a new identity may be given to the DR in the LTDP system.

Altogether it is a crucial phase, since during the ingestion all the authenticity evidence about the pre-ingest life of the DR must be collected, accepted and checked by the LTDP system, and becomes, according to the OAIS reference model, part of the PDI (Preservation Description Information) of the AIP (Archival Information Package).

In the model the following two events are considered in this phase:

- **SUBMIT:** a DR is delivered by the keeping system where it is stored (producer) to a LTDP system;
- **INGEST:** a DR delivered from a producer is ingested by the LTDP system and stored as an AIP.

Even in a minimal situation, as long as a clear distinction between keeping and preserving is done, as it should be, both the above events occur. Thus providing precise guidelines on which evidence should be included in the SIP and how it should be structured is a crucial requirement to ensure interoperability.

3.3 Long Term Digital Preservation (LTDP) Phase

This phase begins when the DR is delivered to a LTDP (Long Term Digital Preservation) system and goes on as long as the DR is preserved. During this phase, the DR may undergo several kinds of transformations, that range from format migrations to changes of physical support, to transfers between different preservation systems.

The OAIS is here considered the reference model. According to the OAIS, many activities are carried out in connection with each of these events, but the model will focus here on the sole aspects related to authenticity and provenance of the DR and on the information (authenticity evidence) that has to be gathered and preserved in the PDI (Preservation Description Information), and more specifically in the Provenance, Context and Fixity components.

Analyzing this phase many possibilities have to be considered: the possibility of transfers between LTDP systems, which is very likely to happen in the long run, and the possibility of changes in the structure of the preserved DRs (integration, aggregation etc.), that routinely happens in the health care sector, since records must enter

preservation as soon they are created and still there may be later the need to introduce corrections. The resulting set of events is then:

- **LTDP-AGGREGATE:** one or several DRs stored in different AIPs, are aggregated in a single AIC;
- **LTDP-EXTRACT:** one or several DRs which are extracted from an AIC to form an individual AIPs;
- **LTDP-INTEGRATE:** new information is added to a DR already stored in the LTDP system;
- **LTDP-MIGRATE:** one or several components of a DR are converted to a new format;
- **LTDP-DELETE:** one or several DR, preserved in the LTDP system and stored as part of an AIP are deleted, after their stated preservation time has expired;
- **LTDP-TRANSFER:** a DR stored in a LTDP system is transferred to another LTDP system.

4 Authenticity Evidence Records

When giving the guidelines that should be followed to ensure interoperability on authenticity among keeping and LTDP systems, beside providing a precise definition of the event, the crucial point is to specify which controls should be performed, which evidence should be collected and how it should be structured.

In the model each event is represented according to an uniform schema:

- the *agent*, i.e. the person(s) under whose responsibility the transformation occurs;
- the *input*, i.e. the preexisting DR(s) that are the object of the transformation, if any;
- the *output*, i.e. the new DR(s) that are the result of the transformation (possibly new versions of input DR(s));
- the *authenticity evidence record*, i.e. the information that must be gathered in connection with the event to support the tracking of its authenticity and provenance.

As the DR progresses along its lifecycle through a sequence of events, an incremental sequence of *authenticity evidence records* is collected by the systems where the DR is kept or preserved, and strictly associated to it. From a practical point of view, an authenticity evidence record is a structured set of information, according to our proposal an XML file of predefined structure, which is strictly related to a given event. At any given stage of its lifecycle a DR brings with it, as part of its metadata, a (temporally) *ordered sequence* of such records, to document all the transformations the DR has undergone and to allow to assess its authenticity and provenance.

Authenticity evidence will follow the DR when it is transferred between different systems, and will accompany it along all its lifecycle. Thus, to ensure interoperability, it is necessary to standardize the way the authenticity evidence is collected and structured. To this purpose existing standards should be accurately considered, as for instance the Open Provenance Model (http://openprovenance.org).

At the moment – as already mentioned in the introduction – the model developed in the framework of the APARSEN project [10] , and here presented, should be considered only as a preliminary step in that direction. Nevertheless, as it turned out from some preliminary practical experiences, it provides a sound basis to derive more detailed operational guidelines and to improve in a significant way the current (and often very limited) practices in managing authenticity and provenance in keeping and preservation systems.

The following subsections discuss a few examples from some events from the core set discussed in sect. 3. For a more detailed discussion one should refer directly to the project documentation.

4.1 SUBMIT

A submit occurs when a DR is moved from a keeping system to a LTDP system. The submit needs to be authorized by the owner of the DR, and involves also the responsibility of the administrator of the keeping system and of the administrator of the LTDP system.

A submission may be considered as the sequence of two steps: i) preparing in the keeping system the DR for shipping; ii) receiving and accepting the DR in the LDTP system. As a consequence, two distinct new versions of the DR are produced: DR' which is kept in the keeping system, and DR'', that is accepted in the LTDP system.

As two different and independent systems are involved in the submission, the keeping system and the LTDP system, the corresponding authenticity evidence record must contain the evidence produced, and conveniently authenticated, by the administrators of both systems. Accordingly there will be two distinct authenticity evidence records, generated and preserved in the two systems.

- **Agents:**
  - owner: the physical or juridical person who originally created the DR;
  - keeping system administrator: the person who submits the DR.
  - LTDP system administrator: the person who accepts the submitted DR.
- **Input:** any DR in the keeping system
- **Output:**
  - DR': the new version of the DR which is kept in the origin system
  - DR'': the new version of the DR, accepted and ready for ingestion.
- **Authenticity evidence record:**
  - *Keeping system*
    - Event type: submit
    - Identification data of the LTDP system
    - Date and time the DR has been prepared for submission
    - Identification and authentication data of the owner of the DR who has given the authorization for the submission
    - Identification and authentication data of the keeping system administrator
    - Evidence that the DR has been received and accepted by the LTDP system
    - Digest of the DR authenticated by the keeping system administrator

- *LTDP system*
  - Event type: submit
  - Identification data of the keeping system
  - Identification data of the LTDP system
  - Date and time the DR has been received from the origin system
  - Identification and authentication data of the LTDP system administrator
  - Assessment by the LTDP system administrator on the delivery of the DR:
    - Identification and authentication of the keeping system
    - Trustworthiness of the data channel used for the transfer
    - Integrity check performed on the digest received from the keeping system
  - Digest of the DR authenticated by the LTDP system administrator

4.2 LTDP-MIGRATE

To migrate an AIP or an AIC means to change the data format of one or several of their components. This is generally triggered by technical obsolescence, but may be as well the result of new policies adopted by the LTDP system on accepted formats. As a result of the migration a new version of the DR(s) is generated, which should preserve its intellectual content, despite the format migration. The most delicate part of this transformation, is to verify that the integrity of the individual DR has been maintained, i.e. that its intellectual content has not changed. Migration may occur both in the pre-ingest and in the LTDP phase, we are considering here the latter case.

- **Agents:**
  - LTDP system administrator: the person responsible of performing the migration
- **Input:** one or several DRs contained in an AIP or in an AIC
- **Output:** a new version of the AIP or AIC
- **Authenticity evidence record:**
  - Event type: migration
  - Date and time the migration has taken place
  - Identification data of the LTDP system
  - Identification and authentication data of the system administrator
  - Digest of the new version of each affected DR after the migration
  - Statement, for each migrated DR, that the intellectual content of the DR has not changed, specifying also the criteria adopted to make the assessment
  - Digest of the new version of the AIP produced by the migration

5 Case Study Analysis

As part of the activities carried on in the APARSEN project, a case study analysis has been performed to check the validity of the model and to see how it specializes on several specific environments [11].

Four case studies have been selected, to cover a reasonable variety of situations:

- a health care data repository,
- two repositories of experimental scientific data,
- a repository of social science data.

Each case study is organized in two parts:

- *What is done right now*. A description and analysis of the *current practices* adopted in the management of the specific repository. The first step is understanding the meaning of authenticity and provenance for the designated community, identifying the main *events* in the DR lifecycle, the transformations the DRs undergo and their impact on authenticity and integrity. Next step is to analyze what is currently done about that, i.e. how DRs are delivered by producers, which controls are performed, which authenticity evidence is collected, etc.
- *What should be done*. That means applying the methodology and the guidelines we propose to the results of the analysis of the current practices, i.e. fitting the lifecycle events into the *core set* of events we propose, identifying the controls that should be done and the authenticity evidence that should be collected, and sketching the improvements one should introduce to correctly manage authenticity and provenance.

We briefly discuss in the following subsections two of the case studies. Due to space limitations the presentation is restricted to the main highlights. For a more detailed account one should refer directly to the complete report that has been published as a deliverable of the APARSEN project [11].

In both cases our model has proved to be effective, since the events in the current situation have clearly mapped into our core set of events, and the structure we propose to represent the events has shown to be adequate. Moreover it has been helpful in formally documenting the workflow and in identifying deficiencies in the management of authenticity evidence.

5.1 Repository of the Public Health Care System in Vicenza, Italy

This study deals with several types of DRs, mainly test results (files in DICOM format and more) and medical reports (digitally signed by physicians), each type of DR being handled by a separate workflow. All records are sent to the repository shortly after their creation and managed according to the Italian rules on LTDP, which are very specific and mostly centered on digital signatures and certified timestamps, and mandate to collect many DRs in a single large batch (called Preservation Volume).

We refer here about the workflow of *studies* (i.e. sets of diagnostic images), which involves in the pre-ingest phase several systems under different responsibilities: Modalities (imaging devices) and local and central PACS (Picture Archiving and Communication Systems) that act as keeping systems in the medical structures. The ingest phase involves a preservation system called Scryba which is compliant with the Italian regulations and the OAIS model. According to our model we could clearly identify in the lifecycle the following events:

- **CAPTURE:** studies are generated by modalities and captured by local PACS;
- **TRANSFER:** studies are transferred from a local PACS to the central PACS;
- **SUBMIT:** a SIP is prepared for each study and is moved from the central PACS to the preservation system Scryba;
- **INGEST:** an AIP is generated for each SIP; the process includes some controls on provenance and integrity, generating the PDI from metadata (both explicit and extracted from the DICOM file) and adding a certified timestamp;
- **AGGREGATE:** several AIPs are aggregated in a single AIC (Archival Information Collection) which corresponds to a Preservation Volume.

According to our analysis the management of the authenticity along the lifecycle is rather reasonable, due to the compliancy to the quite detailed national regulations, but a few improvements have been suggested:

- in the pre-ingest and ingest phases the responsibilities for local and central PACS should be explicitly documented in the authenticity evidence records (AER);
- further controls should be introduced in the ingest phase (integrity checks in the transfers) and the outcome of all controls should be recorded in the AERs.

5.2 Social Science Data Repository at UK Data Archives

The Archive acquires data from a variety of producers in the academic, public, and commercial sectors, providing continuous access to these data, in a relationship which is based on a network of confidence with the stakeholders. The DR lifecycle is substantially different from the previous case and is concentrated on the ingest and the LTDP phases. According to our model we could clearly identify in the lifecycle the following events:

- **SUBMIT:** a SIP, prepared according to the submission agreement, but with a very large degree of variety in its structure, is submitted by the producer to the Archive;
- **INGEST:** a complex transformation that may require the manual intervention of specialized teams to normalize the structure of the information package (and the data themselves) to meet the Archive standards;
- **MIGRATE** and **DELETE:** two additional events, that correspond to transformations in the process to be implemented.

Although the workflow is currently based on well devised and well documented procedures, and complies with international standards, referring to our model during the analysis has proved helpful in identifying a few problems that should be addressed:

- part of the authenticity evidence is currently not included in the SIP, but derived from data deposit forms and agreements: it should instead be collected by the Producers, structured according to detailed specifications and incorporated in the SIP;
- some of the transformations that are currently performed by specialized teams during the ingestion may affect the authenticity of the preserved DRs since the responsibility of the producers cannot be properly documented; according to the

OAIS model the only clean way to fix the problem could be to require the producers to normalize the data themselves before preparing the SIP, possibly providing them with assistance from the specialized teams, if they need it.

References

1. Giaretta, D.: Advanced Digital Preservation. Springer, Heidelberg (2011)
2. Giaretta, D., Matthews, B., Bicarregui, J., Lambert, S., Guercio, M., Michetti, G., Sawyer, D.: Significant Properties, Authenticity, Provenance, Representation Information and OAIS. In: IPRES 2009: Proc. of the Sixth Int. Conference on the Preservation of Digital Objects, California Digital Library (2009), http://www.escholarship.org/uc/item/0wf3j9cw
3. InterPARES Project, Authenticity Task Force: Authenticity Task Force Final Report (2001), http://www.interpares.org
4. Factor, M., Henis, E., Naor, D., Rabinovici-Cohen, S., Reshef, P., Ronen, S., Michetti, G., Guercio, M.: Authenticity and Provenance in Long Term Digital Preservation: Modeling and Implementation in Preservation Aware Storage. In: First Workshop on the Theory and Practice of Provenance, TaPP 2009, San Francisco (2009), http://www.usenix.org/event/tapp09/tech/full_papers/factor/factor.pdf
5. InterPARES (International Research on Permanent Authentic Records in Electronic Systems), http://www.interpares.org
6. CASPAR Project - Cultural, Artistic and Scientific Knowledge for Preservation (2006-2009), http://www.casparpreserves.eu (access and retrieval)
7. Open Archival Information System (OAIS) – Reference Model, ISO 14721:2003 (2003), http://public.ccsds.org/publications/archive/650x0b1.pdf
8. CCSDS: Reference Model for an Archival Information System–OAIS. Draft Recommended Standard, 650.0-P-1.1 (Pink Book), Issue 1.1 (2009), http://public.ccsds.org/sites/cwe/rids/Lists/CCSDS%206500P11/CCSDSAgency.aspx
9. APARSEN Project – Alliance Permanent Access to the Records of Science in European Network (2011-2014), http://www.alliancepermanentaccess.org/index.php/current-projects/aparsen
10. APARSEN Project: Deliverable D24.1. Report on Authenticity and Plan for Interoperable Authenticity Evaluation System (2011)
11. APARSEN Project: Deliverable 24.2. Implementation and testing of an Authenticity Protocol on a Specific Domain (2011)
12. ISO RM 15489-1:2001 Information and documentation – Records management. Part 1: General
13. ISO 23081-1:2006 Information and documentation – Records Management Processes – Metadata for Records
14. UN/CEFACT: Business Requirements Specification. Transfer of Digital Records, Version 1.0 (2008)
15. DLM Forum: MoReq2 – Model Requirements for the Management of Electronic Records (2008), http://www.moreq2.eu
16. DLM Forum: MoReq2010 - Modular Requirements for Records Systems (2011), http://moreq2010.eu