CHALLENGES TO LONG TERM DIGITAL PRESERVATION A GLIMPSE OF THE ITALIAN EXPERIENCE

Patrizio Campisi, Emanuele Maiorana*, Enrica Massella Ducci Teri**, Alessandro Neri**

*Dip. Ingegneria Elettronica,
Università degli Studi Roma Tre
via della Vasca Navale 84, I-00146 Roma, Italy
(campisi, maiorana, neri)@uniroma3.it

**CNIPA
Centro Nazionale per l'Informatica
nella Pubblica Amministrazione
via Isonzo 21b, I-00198 Roma, Italy
massella@cnipa.it

ABSTRACT

In this paper an overview of the challenges to long term preservation of digital objects is given. We highlight threats, which can be posed by humans, hardware/software, environment and institutions to long term digital preservation systems, with specific emphasis to security threats. Some technological solutions are described, and the Italian experience on long term digital preservation is briefly described.

Index Terms— Digital preservation, Security, Privacy,

1. INTRODUCTION

The capability to preserve information is a necessary condition to make our cultural heritage available to the next generations. In the last decades, with the always decreasing cost of high performance computers, the advent of high speed networks, the widespread of compact media supports and low cost digital devices like cameras, video cameras, scanners, etc., an enormous amount of information in digital form has been generated. Moreover, the need to make "analog" resources such as ancient books stored in national libraries, paintings, sculptures, handcrafts stored in museums, and so forth, available to the maximum amount of people, requires first to perform digitalization and then to store the produced digital records. This necessity has also raised the interest of UNESCO, which has developed a strategy for the promotion of digital preservation, formalized in the "Charter on the preservation of the Digital Heritage", adopted at the 32nd session of the General Conference of UNESCO (17 October 2003).

Without being exhaustive, among the projects which have been and are being carried out on digital preservation, we can cite the ERPANET[1] (Electronic Resource Preservation and Access Networks) network (2001-2007) dedicated to design of best practice and skills development in the area of digital preservation of cultural heritage, the InterPARES[2] (International Research on Permanent Authentic Records in Electronic Systems) project, which has been developed in three phases: the first, InterPARES1 (1999-2001), focused on the design of technological solutions to ensure the authenticity of records stored in databases; the second phase, InterPARES2 (2002-2007), dealing with the issues of authenticity, reliability and accuracy of long-term stored records; the third phase, InterPARES3 (2007-2012), aims at the creation of small and medium-sized archives, built upon the the findings of InterPARES1 and InterPARES2, while developing education programs. Moreover, it is worth citing the European Network of Excellence on digital libraries DELOS [3] (2004-2007), which focuses on the formats which can be employed for digital preservation, and deals with the automatic extraction of metadata for information retrieval, the European Project CASPAR [4] (Cultural, Artistic and Scientific knowledge for Preservation, Access and Retrieval), (2006-2009), which focuses on the definition of models and tools for the preservation of scientific and cultural documents, the European Network of Excellence DPE[5] (Digital Preservation Europe), (2006-2009), dedicated to the definition of systems and technologies for long-term management of digital material, the European Project PLANET [6] (Preservation and Long-term Access through Networked Services), (2006-2009), for the preservation of e-government documents, the EU large scale integrating project SHAMAN[7] (Sustaining Heritage Access through Multivalent Archiving), (2007-2011), whose goal is to develop the systems and tools for long term (more than 1 century) digital preservation. Besides the cited projects many others have been and are currently under development at a national level.

Digital preservation involves both bit preservation and logical preservation. On one side, at the bit level, there is the necessity to preserve the digital object. On the other side, at the logical level, there is the need to preserve, in the long run, the document usability. However, long term preservation

[1] http://www.erpanet.org
[2] http://www.interpares.org
[3] http://www.dpc.delos.info
[4] http://www.casparpreserves.eu
[5] http://www.digitalpreservationeurope.eu
[6] http://www.planets-project.eu
[7] http://www.shaman-ip.eu

978-1-4244-3298-1/09/$25.00 ©2009 IEEE

of digital data is a very challenging task since it is strictly dependent on the available technology. In fact, when new technologies are introduced, the older ones are discontinued, making very difficult, if not impossible, to retrieve the information relying on obsolete technologies. We also need to face the obsolescence of file formats, both malicious and non intentional attack, and the volatility of host organizations. Moreover, there is also the need to guarantee the authenticity and the integrity of the stored documents, and to allow the access to only authorized users. All these requirements make the preservation of digital information a much more complex problem than that of analog media [1, 2]. The choice of the most effective long term preservation technique depends on several factors like technological issues, cost of retaining information, end users needs, among the others.

In this paper a general overview of the challenges to long term digital preservation is given. Specifically, in Section 2 end users' requirements are outlined, while in Section 3 a broad classification of the main threats is given. In Section 4 and 5 the technical solutions to long term preservation and the main security threats undermining the use of these systems are described respectively. Eventually, in Section 6 the activities carried out at the Italian national level are briefly described.

2. DIGITAL PRESERVATION: USERS' REQUIREMENTS

The design of a digital preservation system must take into account the needs the future end users will have on the stored data [3]. This analysis would help to determine the necessary side information to store together with the data. Although it is quite difficult to predict the needs an end user will have on the stored data, as a basic usability requirement we need to guarantee the same interactions the present users have with the considered data. More specifically, as highlighted in [3]:

- The end user should be able:
  - to get access to the stored digital data;
  - to render the data on the host machine;
  - to understand the content of the stored data;

  without any technical inconvenience;
- The stored document should be authentic, in the sense that it should be the same document that was originally stored, and it should have the same content, functionality and behavior of the original data;
- Some side information should accompany the stored data to explain which software have to be used to render the document, and to give information about the document content and its intended behavior.

3. THREATS TO LONG TERM DIGITAL PRESERVATION

The threats to long term digital preservation can be originated from different sources. Following the classification given in [4, 5], they may be caused by humans, by hardware/software faults, by large scale disasters, and by institutions. Specifically:

- *Human related threats*: users can erase or overwrite data by mistake or they can cancel by purpose some data the utility they don't recognize but at a later moment. Also operators can loose the media supports or they can store them inappropriately. They can cause hardware faults or software failures because of misconduct, like for example inappropriate driver removal, and so forth. Moreover, many internal or external malicious attacks, like data removal, data alteration, data theft, denial of service, and so forth, can be intentionally perpetrated by people on digital data storage centers;
- *Hardware/software related threats*: hardware components may fail, temporarily or permanently. Software may be affected by bugs and the support can be discontinued. Hardware systems can become obsolete. This implies that it may result extremely difficult to make a given system communicate with others. Storage media readers and writers can become obsolete as well as the employed media supports. Storage media are not completely reliable over long period of time. In fact, they are prone to errors which can accumulate thus making the support completely unusable. Therefore, a wise selection of the storage media for long time preservation has to be performed [6], and special attention for handling and storage of removable media has to be put in place [7]. Software can become obsolete as well. Therefore, either the data which have been stored using those systems cannot be accessed anymore, or the data bits can be read, but the associated content cannot be any longer interpreted. Formats can become outdated and therefore unusable. Methods to counteract hardware and software obsolescence are described in Section 4. Eventually, the data to preserve are ususally stored together with metadata, which include side information like the authors of the content, the software necessary to get access and to manipulate the data, the keys to decrypt the data if encrypted, and so forth. It is therefore evident that the necessity to preserve metadata is as strong as the necessity to preserve the data themselves, and that all the hardware /software threats which can affect the metadata are the same affecting the data;
- *Environmental dependent threats*: natural disasters or conflicts can pose dramatic threats to archival sites;

- *Institutional dependent threats*: the organizations which have data to be preserved, but whose main activity is not data preservation, have to face a complex budget planning for maintaining their archives, and in most cases the budget allocation is very limited. Moreover, institutions can change goals over time or they can go bankrupt. This poses serious threats to the storage systems which can be lost, damaged, left without documentations, and so forth.

It is worth pointing out that the aforementioned threats can derive by multiple causes, therefore the given classification is not strict.

4. TECHNIQUES FOR DIGITAL PRESERVATION

Many techniques have been recently proposed for the purpose of digital preservation. Specifically, we can identify two major preservation strategies [2]:

- Preservation of technological environment:
  - technology preservation;
  - technology emulation.
- Defeat technological obsolescence of file format:
  - encapsulation;
  - information migration.

The aforementioned approaches are described in more detail in the following.

4.1. Preservation of technological environment

Preservation of technological environment aims at preserving the original environment to render the stored data. This goal can be achieved in two different ways.

The first, namely technology preservation [8], consists in making available the whole platform, hardware and software, in order to make the future users able to retrieve and to render the stored documents. However, this approach, which is very conservative, has several drawbacks. It can be appropriate for short term preservation, but when long term preservation must be granted, it is very difficult to guarantee that all the necessary equipment is available and functioning.

The second approach, namely technology emulation [9], consists in designing emulators of the necessary obsolete applications to be run on the up to date systems available. As a basic requirement, the emulators should preserve the digital object as well as its authenticity. This approach requires to preserve the original applications, and to program an emulator to mimic the behavior of the original applications on the new systems, whereas the original hardware is no longer necessary. However, in order to be able to design the emulator, detailed information about the old platform, that is hardware and operating systems, must be known.

4.2. Defeat technological obsolescence of file format

Two different approaches can be used in order to make readable the format of the original file.

The first one, namely encapsulation [10], consists in building a wrapper where, together with the digital object, some side information, like the documentation about the original data format, and all necessary information to provide access to the object, are stored. Of course, this strategy dramatically increases the record dimensions. Moreover, it is not well applicable when original data formats are not well documented.

The second approach, namely information migration [8], consists in the periodic transfer of digital data from one hardware/software platform to the next generation one. Information migration can also be applied to migrate a variety of formats to a limited number of standard formats. This strategy can be successfully employed for short and medium term preservation strategies. However, in the long run, the migration cannot guarantee accurate conversion of the original data to a target file.

In [11, 12, 13], some guidelines for the choice of file formats, of the graphic file formats, and of the image compression techniques are given.

5. SECURITY THREATS TO DIGITAL PRESERVATION

The protection of archived data represents a challenging issue for long term digital preservation [14]. From an information security view point [15], data protection is accomplished when information confidentiality, availability, integrity, and authentication are guaranteed. Since archival storage systems should manage data over long periods of time, each of these properties can be affected by novel threats which are peculiar to the considered scenario.

5.1. Confidentiality

Data confidentiality consists in preventing information disclosure to unauthorized systems or individuals. When sensitive personal information is accessed by unauthorized parties, a significative privacy leakage can also occur.

Data encryption is commonly employed to provide secrecy to the stored information, as in the FARSITE system [16]. However, the security of such approach relies on the inability for an attacker to break the encryption scheme, or to recover the employed key, within the time period during which the document should be kept secret. However, if the archived data have to be stored for an indefinite period of time, the attacker has an indefinite amount of time to break the algorithm. Moreover, technological improvements can lead to a significant reduction of the computational complexity and processing time required to decrypt the stored data by an unauthorized individual.

It is also worth noticing that, in long term storage systems, the encryption key may represent a weak spot, since key loss is effectively equivalent to data deletion. If the keys are stored in the system together with the encrypted data, they must be kept secure for the entire life cycle of the protected information. Encrypting the key using other keys does not solve the problem, which is tackled in [17] by using non-random keys, retrieved on a password based approach.

A *secret sharing* protocol is implemented in the PASIS [18] and POTSHARDS [19] systems, in order to provide confidentiality without employing key based encryption. Within this approach, an adversary has to break more than K shares out of N in order to acquire a secret information. Since no encryption key is required, threshold secret sharing is more robust than key based encryption systems. However, this approach requires a proper register to keep trace of the attempted attacks. In fact, an adversary can corrupt a single share without compromising the whole secret, and try an attack to a different share at a later time. The system can either immediately deal with an attack, or maintain a history of successful attacks, in order to intelligently schedule corrective actions before the secret information is violated.

Data security and confidentiality can also be accomplished by implementing authentication procedures. The PAST system [20] performs this task by employing certificates, registered on smart cards. In this case, a challenge, unique to long-term storage, is represented by the possibility that the legitimate owner of the card might no longer be available when the information is requested. A secure archival storage system should be able to establish relationships among existing and new users and, in case a relationship is proven, providing these latter access to the stored resources.

5.2. Availability

Availability refers to the possibility of accessing the stored information when needed, both to allow individuals to make use of the data, and to exchange them with third party infrastructures. A long-term archival system may be affected by potential issues regarding the localization of the stored information. In fact, due to the enormous amount of archived data, centralized databases are commonly employed to index the location of the stored data. However, although this approach relieves the users from the burden to remember the details regarding the storage of their data, it makes the whole system more vulnerable to potential attacks, since it centralizes a huge amount of information. On the contrary, if the indexes storage is distributed, the indexes can be maintained by the single users, which therefore have more long-term responsibility. However, in this case an attacker that compromises one users index has no access to information regarding other users.

In POTSHARDS [19] files are segmented into units named shards. A user possesses an index which allows locating the shards necessary to rebuild the file. The correct knowledge of the index facilitate the file reconstruction, which can be reconstructed even if the index is lost. Within this respect, a key is not strictly required to recover the data.

Data availability is also subject to legislative interventions which can occur in the long term. Therefore, it can be useful to employ multiple storage repositories, held under multiple legal jurisdictions, to counteract the possibility that data archived in one location are destroyed or modified in ways inconsistent with the owners intent.

It is also worth noticing that the availability of the stored information can be compromised by data migration. Such event can be due to the inevitable failure or obsolesce of hardware, to the necessity of a software update, or even to improve the system security by creating a moving target [21].

5.3. Integrity

When dealing with digital information, the term integrity is used to mean that the digital object has not been corrupted either accidentally or because of a malicious attack. Within the digital preservation scenario, the integrity check should deal with the prevention, tracking and verification of both the changes the digital object undergoes and the changes of the archiving system [22]. Therefore, data integrity should be actively checked at regular intervals.

Integrity checks are often performed by means of scrubbing procedures [21], which periodically scan the data and employ strong hashes to detect potential data alterations. The used hash functions should be properly updated, in order to not allow an attacker to find a collision, and then fooling the integrity control by modifying the original information with incorrect data. However, the use of cryptographic hash function implies that a one bit change in the document produces a very different digest. Since in a long term digital preservation scenario it is very likely that some data changes occur, for example because of migration or emulation, then the use of perceptual hash, which is error tolerant, can be more appropriate. The use of digital watermarking has been recently proposed for integrity check. However, the watermark embedding itself modifies the document integrity unless we consider as original document the watermarked one. Moreover, the watermark should be embedded in each object of the document in order to highlight possible changes to parts of the document. Removal and substitution attack are also of main concern.

Distributed storage systems perform integrity checks by means of challenge/response protocols, in order to verify that each archive behaves properly. Specifically, the strings obtained by binding stored data with a random key and then applying a hash function can be employed to verify the consistency among data stored in different archives, without transmitting the original data. The use of algebraic signatures to perform integrity checks has also been proposed in

[19], where a cryptographic hash is distributed over different archives.

Repair agents at each storage node are employed in [18] to correct data which have been verified to be corrupted. Audit logs are maintained to roll back, within a given temporal window, possible changes committed by a malicious user. A voting mechanism is implemented in LOCKSS [23] to cooperatively check data integrity among different archives, and in case repair the damages that may occur.

5.4. Authenticity

Authenticity refers to the originality of the data, of the data creator, of the sender, and of the receiver. Within the digital preservation scenario, in order to guarantee authenticity, any change of the digital object should be avoided or forbidden. If changes are necessary for the purpose of preservation, they should be traceable and reversible [22].

The use of digital watermarking has been recently proposed to authenticate a digital document. However, the possibility to embed a fake watermark into the digital object creates serious concerns about the proof of authenticity of the digital objects itself. A possible solution could be to use as watermark an object whose authenticity can be verified. Moreover, the use of fingerprints, that is the use of different watermarks for different copies of the same object, makes difficult to perform a comparison among copies as a way to verify authenticity.

6. THE ITALIAN EXPERIENCE IN DIGITAL PRESERVATION

In this Section a glimpse to the activities carried out in Italy, at a national level, for long term digital preservation is given. The governmental Italian organization most involved with long term digital preservation is CNIPA[8], which is responsible for the ICT support to the Italian public administration (PA). Specifically, the digitalization of paper documents and their subsequent storage represents one of the most important activities currently carried out.

According to the Italian legislation (initially established with the law No. 59/1997, and later consolidated with the Presidential Decree 445/2000), the use of electronic document representation is legally valid and relevant for any purpose, both for public administration and for private companies, under the condition that they are certified to be consistent to the original. However, due to several differences in the procedures to state the consistency of paper and digital documents in the private and the public domain, specific technical rules have been established by CNIPA (Regulation 11/2004) for document reproduction and long term preservation in data storage, to guarantee digital document integrity and authenticity. The goals of such regulation can be summarized as follows:

- To simplify all the processes involving digital native documents in the PA;
- To guarantee the access, the reproduction, and the delivery of documents when a preservation protocol takes place;
- To define policies for the security of digital objects, whose integrity and authenticity should be certified by means of digital signatures and time stamps;
- To define policies for handling non-digital documents. The final goal is to preserve, if possible, only digitalized documents which have been certified by the Preservation Manager to be compliant to the original. The Preservation Manager has to define the preservation procedure, the logical and physical security policy, to keep trace of the different platforms used over time, and to verify periodically the document readability.
- To properly reproduce storage media, in order to extend media life and guarantee document readability;
- To definite procedures for the updated of the documents format to new platforms, when a technological update takes place. Within this scenario, a digital signature renewal is required.

The whole digitalization process of documentation, from its production and authentication by digital signature, to its electronic transmission within and outside the PA, and finally to its access and use by citizens and enterprises has become a reality with the adoption of the "Digital Administration Code", the legislative decree n- 82/2005, that unifies all the several existing statements, thus working as a "Digital Constitution" for all public operators in the field of ICT. The Digital Administration Code contains several recommendations and regulations regarding the use of ICT in the PA, and it has both legislative and technical value since, through a series of related decrees, it establishes technical standards for a communication infrastructure that links all government departments and provides standards for certified email. From this point of view, the Code is a good starting point for examining the aspects related to documentation production, organization and conservation within the PA, and to ensure and regulate the availability, management, access, transmission, storage and accessibility of information in digital mode, by using the most appropriate technologies. In order to accomplish these tasks, an inter-ministerial working group has been established by the Minister of Innovation and Technologies in 2004, and renewed in 2007, with the objectives of simplify the actual regulation, verify the impacts of possible initiatives on the PA, and make aware local and national governmental authorities of benefits available from a proper

[8] http://www.cnipa.gov.it/site/it-IT/

application of document digitalization. In order to support the inter-ministerial group, specific technical committees, working on general aspects of the digital acquisition of paper documents or focusing on specific classes of documents, have been constituted. These working groups have produced a law decree draft and attached technical rules for the dematerialization of records generated through the activities of government bodies, with respect to the reorganization of administrative procedures in the digital environment. The term "dematerialization" is a strongly evocative term pinpointing the gradual loss of physical substance on the part of traditionally paper-based government records through replacement with electronic records. It can thus be described as the direct result of both the gradual increase in computerized records management in public and private productive procedures, and the replacement of conventional administrative records with electronic records possessing full legal value. The above mentioned law decree draft, valid for both the public and the private sectors, provides concrete indications for the management and long-term preservation of different types document and related metadata inside an organized document system, also identifying the required media, the recording methods, the formats and the technical solutions to be adopted to maintain document integrity and authenticity. In addition, this decree draft define the role of a professional Preservation Manager, and takes note of the required training, with specific reference to the critical issue of the long-term preservation and the problems raised by the outsourcing of records management. The decree's vision mainly fits with international standards' indications related to long-term document preservation within a defined and organized digital archiving system, in particular with OAIS [24], the ISO reference model for Open Archival Information System, and the European MoReq2[9] (Model Requirements Specification for the Management of Electronic Records) specification, focused on the management of electronic records by an electronic records management system, or ERMS. The first considerations emerging from these regulation activities regard the complexity of the subject matter, which is far greater than expected, due to a huge range of different situations came upon administrative records' management. It seems reductive and misleading to consider dematerialization exclusively in terms of record digitalization. It should instead be viewed as the result of a substantial simplification of processes and procedures and a redefinition of responsibilities throughout the life cycle of administrative records up to the preservation phase, and hence the reengineering of organizational models and the improvement of professional profiles. Further discussion subject is the predominance of legislative problems with respect to technical solution availability, within a framework of new acts and decrees that requires a not simple interpretation and a set of rules that cannot be fully applied. Concerning operational point of view, it appears necessary to activate proposals to increase awareness of legislators, ICT companies and common users, formulating recommendations and guidelines, defining procedures and standards, providing cost analysis in relation to objectives and methods, and creating specific training course plan for technical and administrative personnel. Further activities, associated with the analysis of organizational problems related to electronic record management and its integration within administrative structures, especially regarding responsibilities definition, can regard the spreading of best practices, the sharing of analysis on critical points met during development, the monitoring and assessment of archival tools in digital records management system, and the evaluation of problems regarding the management of "hybrid systems" (paper and digital document preservation within the same archive). Beyond regulation activities, CNIPA main goal is to support public administrations in the effective use of ICT promoting eGovernment projects. Among this action we can mention:

- Project AU.G.U.STO. (Automazione Gazzetta Ufficiale Storica), for the digital acquisition and storage of the historical Italian official journal promulgating approved laws, with documents dated from 1860 to 1946. Ancient official journal digitalization is affected by several problems like curved paper, text skew, deteriorated paper, non standard typeset, too thin paper and double side print, and other kinds of ancient document noises (ink dots, background spots, etc.). However cataloguing, collating and publishing the ancient collections has a positive effect on ensuring their preservation even if using different media and on simple and rapid accessing through the website of rare and old protected documents which are not available as originals for readers, students and researchers;

- Project E-CEDOLINO for the use of public administration employees' electronic pay slips. It gives a useful service to approximately 1.5 million employees of central and local government, who receive their pay slip by email or other communication channels (fax, sms), and can look it up through a website;

- Project DOCAREA for document management and communication among more than 250 local governmental entities. It can be considered a practical example of the principle that back office organization and rationalization are fundamental enablers for improving the quality and variety of the services provided by the PA to citizens and enterprises. The participating Administrations, while preserving their operational autonomy, share technical solutions and best practices covering the entire document flow. Highlights of the project include:

  - realization of a technological and organizational infrastructure for the document management back

[9] http://www.moreq2.eu/

office;

- complete coverage of the document life cycle, from creation as a non-formal document, to transmission to the current archive as formally registered administrative papers, to their preservation in the deposit archive, where they must be kept for 40 years before migrating to the historical archive;
- high performance management of digital documents including their validation according to the current legislation, digital signing, archival and preservation certified mail for internal and external exchanges integration with work flow management systems;
- unique "digital deposit" for long-term preservation of deposit archives of all the involved administrations, in order to minimize the costs and share the investments;

- Regulation pertaining electronic invoice: electronic invoicing, which can significantly cut invoicing costs, is now rapidly developing, as a remarkable result of the growth of electronic commerce. From an organizational point of view, electronic invoicing procedures are able to generate new models of interaction among enterprises, service providers, software houses and banks. The beginning of 2004 represents the turning point for the Italian situation as in two months the legislative framework has been completely changed by a series of fundamental acts that now form the backbone of the Italian way to e-invoicing and e-storage:
  - Ministerial decree of 23 January 2004;
  - CNIPA Regulation n. 11/2004;
  - Legislative decree n. 52 of 20 February 2004-adoption of 2001/115/CE directive.

  In such a scenario, one of the fundamental steps is represented by the identification of a standard "invoice core data model" for document exchange adopting an appropriate XML data structure;

- Regulation related to the automation of administrative procedures related to civil registration system: a specific technical working group has been constituted to analyze objectives and procedures of the civil registration system, with a focus on the operating process management, the civil acts certification, and the civil registers long-term preservation. Due to the requirements complexity, it has been decided to propose a gradual automation process, by using both paper and digital archives at the beginning:
  - the traditional register archive, preserved in each municipality, contains the original documents, thus ensuring the respect of the authenticity and legal value requirements, and guaranteeing long-term preservation;
  - the digital archive, preserved in a unique national center where all municipalities periodically transfer their archives, looks like a "second" original archive, and works as a "digital deposit" ensuring *disaster recovery* and *business continuity* functionalities;

- Email preservation: a document giving a concise but complete account of the main problems connected to e-mail preservation and archiving, and drawing the basic policies and procedures for the PA, has been prepared. E-mail messages have become an increasingly important and strategic resource for each organization: due to the fast growing of their volume, they should be centrally managed, and archived and preserved according to precise and well defined criteria.

In addition to the activities performed by CNIPA, it is worth mentioning the "Fondazione Rinascimento Digitale" (FRD) [10], which seeks to apply innovative information and communication technologies for the definition of standards, methods and tools capable of preserving digital representations of Italian cultural heritage. To this aim, the FRD actively promotes collaborations among the principle research centers in Italy, and proposes initiatives to spread a significative awareness about the capabilities of digital memories and their applications to cultural heritage, like the conference on "Empowering users: an active role for user communities", which will be held in Florence, Italy, in December 2009.

A proposal for the creation of an Italian network dedicated to the preservation of authentic digital records, namely "ReDigit", is currently under review. The proposed network should represent the Italian contribute to the InterPARES3 Project. The ReDigit network should be involved with researches in critical areas (definition of metadata for digital preservation, software requirements, and so on), advanced staff training, and awareness raising on the issues of processing and preserving digital memories.

7. REFERENCES

[1] S.-S. Chen, "The paradox of digital preservation" Computer, vol. 34, no. 3, pp. 24-28, Mar. 2001.

[2] K.-H. Lee, O. Slatter, R. Lu, X. Tang, and V. McCrary, "The state of the art and practice on digital preservation" Journal of Research of the National Institute of Standards and Technology, vol. 107, no. 1, pp. 93-106, 2002.

[10] http://www.rinascimento-digitale.it/indexEN.php

[3] J. Doyle, H. L. Viktor, E. Paquet, "Long term digital preservation - An end users perspective", 2nd International Conference on Digital Information Management, 2007, Vol. 1, 28-31 Oct. 2007, pp. 146-151.

[4] M. Baker, K. Keeton, S. Martin, "Why Traditional Storage Systems Don't Help Us Save Stuff Forever", The First IEEE Workshop on Hot Topics in System Dependability, 30 June 2005, Yokohama, Japan.

[5] M. Baker, M. Shah, D. S. Rosenthal, M. Roussopoulos, P. Maniatis, T. Giuli, and P. Bungale, "A fresh look at the reliability of long-term digital storage", in Proc. of the 1st ACM Sigops/Eurosys European Conference on Computer Systems 2006 (Leuven, Belgium, April 18 - 21, 2006). EuroSys '06. ACM, New York, NY, 221-234.

[6] The National Archives, "Digital Preservation Guidance Note 2: Selecting Storage Media for Long-Term Preservation", retrieved on April 2009, http://www.nationalarchives.gov.uk/documents/selecting-storage-media.pdf

[7] The National Archives, "Digital Preservation Guidance Note 3: Care, Handling and Storage of Removable media", retrieved on April 2009, http://www.nationalarchives.gov.uk/documents/removable-media-care.pdf

[8] J. Garrett and D. Waters, "Preserving Digital Information, Report of the Task Force on Archiving of Digital Information", The Commission on Preservation and Access and The Research Libraries Group, Washington DC and Mountain View CA, May 1996.

[9] S. Granger, "Emulation as a Digital Preservation Strategy", D-Lib Mag. 6 (10), (2000), retrieved on April 2009, http://www.dlib.org/dlib/october00/granger/10granger.html.

[10] A. Waugh, R. Wilkinson, B. Hills, and J. Dell'oro, "Preserving Digital Information Forever", Proc. Conf. ACM Digital Libraries, San Antonio (2000) pp. 175-184.

[11] The National Archives, "Digital Preservation Guidance Note 1: Selecting file formats for long term preservation", retrieved on April 2009, http://www.nationalarchives.gov.uk/documents/selecting-file-formats.pdf

[12] The National Archives, "Digital Preservation Guidance Note 4: Graphics File Formats", retrieved on April 2009, http://www.nationalarchives.gov.uk/documents/graphic-file-formats.pdf

[13] The National Archives, "Digital Preservation Guidance Note 5: Image Compression", retrieved on April l2009, http://www.nationalarchives.gov.uk/documents/image-compression.pdf

[14] M. W. Storer, K. M. Greenan, and E. L. Miller, "Long-term threats to secure archives", in Proc. of the 2nd Int. Workshop on Storage Security and Survivability (StorageSS 2006), Alexandria, VA, pp. 916, October 2006.

[15] H. Bidgoli, "Handbook of Information Security", Wiley, February 2006.

[16] A. Adya, W.J. Bolosky, M. Castro, R. Chaiken, G. Cermak, J.R. Douceur, J. Howell, J.R. Lorch, M. Theimer, R. Wattenhofer, "FARSITE: Federated, available, and reliable storage for an incompletely trusted environment", In Proceedings of the 5th Symposium on Operating Systems Design and Implementation (OSDI), Boston, MA, Dec. 2002.

[17] L. Masinter, M. Welch "A System for Long-Term Document Preservation", Archiving 2006, Ottawa, CA, May 2006.

[18] J.J. Wylie, M.W. Bigrigg, J.D. Strunk, G.R. Ganger, H. Kiliççöte, P.K. Khosla, "Survivable information storage systems", IEEE Computer, Vol. 33, Issue 8, pp: 61-68, Aug. 2000.

[19] M. W. Storer, K. M. Greenan, E. L. Miller, K. Voruganti, "POTSHARDS: Secure Long- Term Storage Without Encryption", in the Proceedings of the 2007 USENIX Technical Conference, June 2007.

[20] P. Druschel, A. Rowstron, "PAST: A large-scale, persistent peer-to-peer storage utility", In Proceedings of the 8th IEEE Workshop on Hot Topics in Operating Systems (HotOS-VIII), pp. 7580, 2001.

[21] Q. Xin, T.J.E. Schwartz, E.L. Miller, "Disk infant mortality in large storage systems", in Proceedings of the 13th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), Atlanta, GA, Sept. 2005.

[22] M. Schott, J. Dittmann, C. Vielhauer, C. Krätzer, A. Lang, "Integrity and Authenticity for Digital Long-Term Preservation in iRods Grid Infrastructure", in Proceedings of the 6th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods, Poznan, Poland, October 2008.

[23] P. Maniatis *et al.*, "The LOCKSS peer-to-peer digital preservation system", ACM Transactions on Computer Systems, Vol 23, No. 1, pp: 2-50, 2005.

[24] Reference Model for an Open Archival Information System (OAIS), CCSDS 650.0-B-1 BLUE BOOK January 2002, retrieved on April 2009, http://public.ccsds.org/publications/archive/650x0b1.pdf