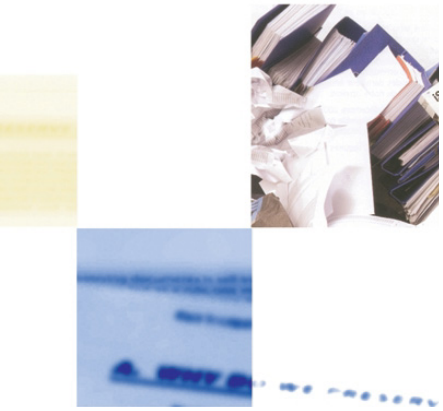


I.R.I.S.
Document to Knowledge™

Image Recognition
Integrated Systems Group S.A.
Professional Solutions

Rue du Bosquet 10
Parc Scientifique de Louvain-la-Neuve
1435 Mont Saint Guibert
Belgium
tel. +32 10 48 75 30
fax +32 10 48 75 40

www.irislink.com

BeLAIIM

icri

SA Stadsarchief Antwerpen

F. Boudrez, H. Dekeyser and Prof. J. Dumortier

Digital archiving: the new challenge?

Digital archiving:

the new challenge?

legal and archival issues

Filip Boudrez (Stadsarchief Antwerpen)
Hannelore Dekeyser and
Prof. Jos Dumortier (ICRI – K.U.Leuven)

I.R.I.S.
Document to Knowledge™

Digital archiving:

the new challenge?

legal and archival issues

Filip Boudrez (Stadsarchief Antwerpen)

Hannelore Dekeyser and
Prof. Jos Dumortier (ICRI – K.U.Leuven)

D/2005/10.484/1
February 2005

Responsible editor: I.R.I.S. Group S.A.

I.R.I.S.
Document to Knowledge™

Image Recognition
Integrated Systems Group S.A.
Professional Solutions

tel. +32 10 48 75 30
fax +32 10 48 75 40

TABLE OF CONTENTS

Part 1: The Legal Framework for Business Archives

Part 2: Electronic Record Keeping

PREFACE

ARCHIVING *or*

How a business problem in combination with increasing strict legislation can motivate organizations to develop successful strategies and competitive advantages.

When man invented writing he also invented archives. This made it possible for him to leave behind traces of his experiences, his discoveries, his fears and his inventions. Philosophy, religion, art and science made strides through the sharing of acquired knowledge written on tablets, on parchment or in books. The invention of printing greatly accelerated this evolution by allowing the diffusion of ideas within a group of elites and later to a population ever hungrier for knowledge.

The invention of archives served as the cornerstone for knowledge. Increasingly vast amounts of more and more specialized knowledge can be passed on from generation to generation. This has modified the challenge: the problem is no longer how to conserve but how to manage, sort and use the information stored in increasingly gigantic databases.

In response, man invented electronic knowledge management. As a result of progress made in the fields of computers and telecommunications, enormous quantities of data can now be handled (conserved, managed and used) electronically. Nevertheless, highly sensitive questions regarding the safety and durability of electronic archives have not yet received completely satisfactory answers.

The question is: Do we have a choice? Can companies and administrations really do without electronic archives? The answer is clearly "No".

Archiving: a key part of company strategy

The creation of civil law and taxes generated the obligation to conserve documents for possible controls of adherence to legal provisions. Since the beginning of this century and in response to numerous cases of accounting and financial fraud in large companies, there has been a concerted effort to reduce the risk of fraud or at least to identify the perpetrators. The "Sarbanes-Oxley Act" is the best example of this movement. Even more recently, the famous "Basel II" rules were laid out in an effort to better ensure the stability of the banking system by better calculating risk before granting credit. Other initiatives have also been taken or are in the works to ease restrictions on the energy sector, regulate polluting gas emission quotas and combat dirty money laundering, etc.

Regardless of the economic situation, we are faced with an exponential increase in the amount of information circulating within our organizations. Though only a fraction can truly be used for business, we are condemned to develop strategies to archive and store this data. Electronic archiving has become crucial and entails the identification of appropriate solutions to related technical problems.

Therefore, while in the past organizations were forced by necessity to electronically archive data useful for their business, they now must also satisfy increasingly broad requirements to follow precise electronic archiving rules. IT departments are no longer the only entities to suffer from this problem. Organizations as a whole in all *business* departments are concerned. Knowledge is the most important asset. It must, therefore, be protected, managed, preserved, circulated, exchanged and made safe. For these reasons, archiving is one of the key issues facing organizations.

More than 10,000 laws and norms form the legal framework regulating archiving in the US. Though the system is not yet as complex in Europe, norms developed in the US have rapidly leaked throughout the world, through subsidiaries of American companies, for example. In addition, discussions to this effect have already taken place at the European Communities level and within most European countries.

There currently exist texts that regulate proof of electronic signature, preservation of electronic documents or even electronic billing. Specific regulations have been implemented in certain sectors such as social security, retirement funds, income tax or VAT declarations, etc. The ISO and AFNOR (French Association of Normalization) have published legal archiving procedures and regulations.

One example of a legislative initiative: the Sarbanes-Oxley Act

The problem of "compliance" is at the heart of this issue. The regulations were designed to define the way in which companies create, store, consult, preserve and archive recorded data (information in various forms) for increasing durations of time. If companies do not comply with these archiving system requirements, heavy fines could be imposed on them.

The Sarbanes-Oxley Act, adopted in July 2002, creates a stringent set of rules aimed at restoring investor confidence lost as a result of various scandals such as those concerning Enron, WorldCom and others. This law is guided by three overall principles: accuracy and availability of financial information, increased responsibility of company executives and independence of auditors. Companies are obliged to rapidly provide access to their accounts and the CEO and CFO must personally certify financial reports. In addition, this law reinforced control measures over every aspect of a company's financial report. Section 404 gives the SEC (US Securities and Exchange Commission) the power to prescribe rules requiring registered companies to include in their annual report filed with the SEC a specific report in which Management attests to the efficacy of internal controls of financial reporting.

The Sarbanes-Oxley Act is applicable to companies, banks and savings associations that file reports with the SEC under section 13(a) or 15(d) of the Securities Exchange Act of 1934. Thus, this concerns all listed companies. The transitory measures will expire the 15th of April 2005 and, thus, the Sarbanes-Oxley Act will come into full effect without exception. On one hand, all non-American companies with activities in the US and that file reports with the SEC must comply with the act for all their activities. On the other, all subsidiaries and branches of American companies throughout the world that file reports with the SEC must also comply. Therefore, to a certain extent, this law is universal.

The Sarbanes-Oxley Act does not define the conditions for appropriate internal control, but the SEC did create an internal control structure (Committee of Sponsoring Organizations or COSO) that meets its criteria for evaluation and development of controls. COSO defined five components of effective internal control: control environment, risk assessment, control activities, information and communication and, lastly, monitoring. Since the 26th of April 2003, companies work with independent verification committees to monitor the verification process. These independent committees are authorized to receive complaints from shareholders or employees concerning the company's accounting procedures and verification procedures.

Concerning the control environment, the COSO stresses the importance of the assignment of authority and responsibility: the management of identities and access is crucial. In the area of control activities, the COSO requires company management to define the policies, procedures and specific actions necessary to manage the risks associated with the specific controls. Management must evaluate the design and operational efficiency of these specific controls to deal with the risks they intend to address.

The COSO lets companies define the control measures specifically applicable to IT. Several companies based their measures on COBIT (Control Objectives for Information and related Technology) published by the IT Governance Institute. These guidelines describe in detail the activities required for the evaluation of IT controls in order to comply with the Sarbanes-Oxley Act. The COBIT controls can be classified into four categories: planning and organization, acquisition and implementation, supply and support and, lastly, monitoring.

A key element of the control of supply and support is the "Ensure Systems Security" that provides controls to protect information against unauthorized use, divulgation or modification as well as against damage or loss. This is achieved through logical access controls reserved for users authorized to access the systems, data and programs they need. COBIT defined 22 different control objectives ranging from firewalls to virus protection and from reactions to incidents to the management, authentication and authorization of users. Company management must then thoroughly evaluate the controls, including the levels of access to the computer system, to be able to certify that the control of access to sensitive financial information is sufficient and effective.

The Sarbanes-Oxley Act thus affects information systems on two levels:

- use of computers for management and financial control: each actor must be able to save data (bottom-up input) and management must be able to perform completely transparent controls (top-down visibility),
- requirement to certify computer system safety.

The opportunity to create a competitive advantage

It will certainly be a challenge for companies to comply with the requirements of the Sarbanes-Oxley Act and other current regulations.

However, several existing tools could serve as aids in this process:

- intelligent, indexed electronic documents allowing “full text” or fuzzy searches,
- scanning of incoming paper mail, indexation and integration into an electronic document management system,
- text recognition (OCR) from archived documents in image form to allow optimal searches,
- electronic management of billing or automatic recognition of paper bills,
- electronic document and workflow management so that the stage of the processing process in which a file is located can be identified at any time,
- archiving of e-mails, scanned mail and work files according to stringent procedures using reliable systems whose configuration meets standards defined by authorities,
- effective, highly regular backups.

Several of these applications improve speed and accessibility, among other things, for users and/or management. This means improved productivity.

The goal of this book is not to describe all the individual existing applications, but it is important to describe the role of archiving in the larger context of computer architecture and, more generally, of *business* needs.

As technology evolves, laws are adapted

I.R.I.S. has been leading efforts to rethink and improve archiving for nearly twenty years. Offering products and solutions for scanning, text and document recognition, electronic document content and lifecycle management, and information archiving and storage, I.R.I.S. has been helping organizations to improve their operations and gain a most often crucial competitive advantage.

We are, thus, well placed to evaluate the considerable acceleration of technical progress made in our field. Servers have reached a level of performance that would have been unimaginable only five years ago. The response times and data capacity of digital storage systems are mind-boggling. The capacity of software to handle information has also improved at a constant or even exponential rate.

Like in many scenarios where reality evolves faster than fiction, laws have been slow to keep up with the breakneck speed of evolution of these technologies. The team led by Professor Dumortier in the Interdisciplinary Centre for Law and Information Technology (ICRI) has collaborated in the creation of several legislative initiatives at the European level. Their work has given us a view of the current situation in the area of computer law regulating archiving issues. The DAVID system developed by the Archives of the City of Antwerp (Stadsarchief Antwerpen) is certainly one of the most successful electronic archiving systems. Its implementation by the team of Mr. Boudrez provided us with extremely enriching practical feedback.

Through the publication of this work, we hope to help heighten awareness about the fact that as technical solutions continue to evolve, the legal framework is adapted to allow organizations to define the guiding principles of a policy for safety and competitiveness. This book presents an up-to-date, in-depth view of electronic archiving. What is truly possible? What are the legal constraints? How does a complex archiving system really work? What are the pitfalls and opportunities?

We'd like to thank the BeLAIIM (Belgian and Luxembourgian Association for Information and Image Management) for their support of this initiative and their contribution to its success.

Happy reading!

Etienne Van de Kerckhove
CEO I.R.I.S. Group

A. WHY DO WE PRESERVE DOCUMENTS?

Preservation is "the practical task that consists of keeping documents intact for future use". In preserving documents, we want to make and keep the information that they contain available for the future. There are many different reasons for preserving documents. In the business community, documents are mainly preserved for legal reasons. Documents are kept because we are required to do so by law or because we are obliged to do so by virtue of a contract, or for the sake of their value as evidence. For society in general, historical and scientific research are two additional reasons for preserving documents.

1. EVIDENCE LAW

One of the paramount reasons for preserving documents is self-interest. The law grants many rights to natural and legal persons, but as a rule, one must be able to demonstrate that the conditions for obtaining these rights have been fulfilled. If someone wants to assert his rights on the basis of an agreement, he must first demonstrate the existence and validity of the agreement. If someone wants to hold another person liable for an error, he must first demonstrate that there is an error, that harm has been suffered and that there is a causal relation between the two.

No one can predict whether and when a dispute will arise about the legal rights that he claims to have. Therefor it is important to preserve all documents that could support these claims. Archiving is thus inextricably connected to the law of evidence.

The preservation period as required by the law of evidence is demarcated by the statute of limitations established by civil law. As such, the statute of limitations does not directly oblige anyone to preserve documents. However, one consequence of the statute of limitations is that obligations become unenforceable after a certain period of time has lapsed. Therefor these rules indirectly determine the period within which a right can be enforced in court, and thus the period during which the necessary evidence must be preserved. Anyone who destroys his evidence prematurely will have to bear the consequences when he can no longer demonstrate his rights before the court.

The limitations period for personal actions was recently reduced from thirty years to ten years (art. 2262 bis §1 of the Belgian Civil Code). Personal rights are those rights that can be asserted against a person, for instance the right to have a debtor perform actions such as providing payment for merchandise or a demand for compensation from a person who is liable. For legal actions based on civil liability the term is reduced to five years. However this reduced term only starts running when the injured party becomes aware both of the damage suffered and the identity of the person liable for it. In case these two conditions are never met, the liability claims are extinguished twenty years after the incident occurred that caused the damage. For an action *in rem*, claims attached to movable or immovable goods, the limitations period is thirty years (art. 2262 of the Belgian Civil Code). In all these cases, the term is extended under certain circumstances, for instance when one of the parties is a minor, or by certain acts, such as a notice of default or the institution of legal proceedings.

The law of evidence contains the fundamental rules according to which all documents are judged in all areas of the law. Insofar as no specific rules apply, the law of evidence determines the form that documents must take from a legal perspective. For this reason, a general overview of the law of evidence will be given in the first chapter.

2. LEGAL OBLIGATION TO PRESERVE DOCUMENTS

The Public Records Act imposes a general obligation on the public sector to preserve their records[1]. There is no equivalent general obligation for the private sector.However, businesses must take into account many specific and industry-related obligations to preserve documents. Corporations and merchants are obliged to keep accounts to suit the nature and size of their business and to keep these for 10 years. Employers must store a wide variety of social documents. Taxpayers are obliged to retain all the documents needed to determine their taxable income.

The rules on accounting are mainly intended to safeguard the rights of third parties. When entering into important transactions, the future creditor can consult the company's annual financial statement. The other preservation obligations imposed on organisations are intended to provide the government with a verification tool. The tax authorities have extensive powers to examine the accounting books to determine whether declared income agrees with true income.

All these specific regulations impose their own requirements on the form in which documents must be drafted and preserved.

3. CONVENTIONAL OBLIGATION TO PRESERVE DOCUMENTS

Sometimes there can be a contractual basis for storing documents. Companies can entrust the management of their archives to a specialized firm with which they enter into a custody agreement[2]. The custodian must then return the documents to the depositor at his first request.

B. THE ORGANIZATION OF THE ARCHIVE

Every organization must develop an archiving policy with practicable archiving procedures to reach the objectives described above. Archiving only makes sense when the documents retain their authenticity. It must be possible to evaluate the authenticity and reliability of documents when they are requested from the archive for reuse. A document is authentic if it is in reality what it purports to be.

A document's authenticity is determined on the basis of its integrity and identity. The identity of a document can be determined from its origin and context. All the information that is needed to determine the authenticity must be preserved in the metadata accompanying the record in the archive. Metadata include the author and/or the person responsible for the document, the date, the (business) process within which it was created or received, etc. Archiving is first and foremost a practical task: in order to preserve a record, the appropriate technical and organizational measures must be taken.

The archival policy and the entailing archival procedures must take into account the modalities and limitations that the law imposes. Privacy regulations and copyright have a special impact on all aspects of archiving. The right to privacy limits the data that may be included in the archive. Any personal information in the archive must be stored carefully and may not be handed over to third parties as a rule. The inclusion in the archive of works protected by copyright requires, in principle, the permission of the copyright holders, as does modification and further distribution of the work.

C. *DIGITAL DOCUMENTS: DEFINITION OF THE PROBLEM*

Today, paper is still the medium of choice for the preservation of documents. Paper's long life cycle and relatively simple storage methods do, indeed, make it very suitable for the long-term preservation of many types of information.

But using paper also has disadvantages. A lot of storage space is needed to stock paper; which imposes substantial costs on companies. The legal obligation to preserve documents often confronts corporations with serious archiving problems due to lack of space. Moreover, retrieving information from paper archives is a labour-intensive and therefor expensive endeavor. Paper does not allow information to be processed rapidly and efficiently.

For these reasons more and more companies are looking to switch to an electronic document management system to manage their documents. Many are considering replacing original paper documents with electronic copies, in order to reduce the need for storage space. Extensive search functions help to ensure that relevant information is rapidly available.

The advantages of electronic over paper storage are not the only reasons companies have for using a digital archiving system. Companies are increasingly confronted with documents that originate in a digital form. Today, most documents in a company are produced electronically through a variety of computer applications. The exchange of information between business partners is also often handled electronically, so that an electronic version is the only version that exits. Anyone wanting to do business quickly and cheaply without too many formalities uses internet technology to keep in contact with customers and/or suppliers. Computer applications are widely used to steer and support internal operational processes. All this has led to a dematerialization of information transfer.

Today, many digital documents are still printed and then filed in paper form. This practice does little to lower costs and is gradually becoming untenable. Sophisticated electronic documents, such as databases and multimedia objects, can not be printed to paper in a meaningful way.The deployment of electronic document management and archiving systems is the way forward.

However, several legal obstacles can stand in the way of an optimal use of an electronic document management system. Prior to the implementation of such a system, the limits posed by law on the use of electronic documents must be researched and applied to the company's circumstances.

A classic legal problem relating to electronic information has to do with the question of evidence. Reasonable certainty must exist that a court will accept electronic information as evidence when a dispute arises. The law of evidence is a determining factor for the way in which we archive documents. In addition, other legal rules that could impede the creation and/or preservation of legally relevant, electronic information should be taken into account. The Electronic Commerce Act seeks to put an end to the obstacles that currently exist for the conclusion of contracts online.

Beside the law of evidence there are special stipulations in tax law and accounting law, medical law and social law that each apply to one specific type of document. These stipulations often deviate from the law of evidence with respect to the method and term of preservation. However, these sectoral rules often only concern the relation between the taxpayer, the doctor or the employer with the government. With regard to others, it is often still evidence law that provides guidance for the preservation of documents and the evaluation of their legal value.

D. GENERAL FRAMEWORK: THE LAW OF EVIDENCE

1. INTRODUCTION

Evidence can be defined as "demonstrating the accuracy of a fact or of the reality of a legal transaction when there is a dispute about this between the parties"[3]. In Belgium a closed evidence system applies to civil cases, as laid out by the chapter entitled "Evidence of Obligations and Evidence of Payment" of the Civil Code.[4] This means that the legislator only accepts as proven in court that for which certain types ofcredible evidence has been presented[5]. More specifically, this refers to written evidence, the testimony of witnesses, circumstantial evidence, the parties' admission and the oath. The civil evidence rules apply in all areas of law insofar as a contract or another law do not explicitly provide otherwise

The Civil Code establishes a hierarchy of the various types of evidence because the legislator considers some types of evidence more credible than others. The signed document plays a particular role here because it fulfils the following functions:

- it is possible to *identify* the author
- the document's *integrity* is guaranteed
- the author has *appropriated* the content of the document.

Because of the presumed reliability of signed documents, the legislator requires that important agreements with a value in excess of 375 EUR be substantiated with a signed document. Traditionally, this refers only to a paper document signed by hand. Since the introduction of the law on the electronic signature, an electronically signed document is also one of the options. In principle, no other forms of evidence are admissible for this type of agreement.

The party who has a signed document is in a strong position because of its special evidential value[6]. After all, the law stipulates that the court may not doubt the truth of a signed document presented by one party unless the opposing party can present another document in rebuttal. In presenting a signed document one proves the claim instantly, as it were. This is an important difference from a normal (unsigned) document, which may be admissible evidence for claims with a value under 375 EUR, but the credibility of which the court may evaluate for itself. The signature of the party against whom one submits a document makes the document a very credible article of evidence.

2. A DOCUMENT SIGNED BY HAND

The handwritten signature has long held a central position in civil law of evidence and in many respects it served as model for the electronic signature. That is why we will pause to discuss traditional paper evidence before turning to electronic documents.

Traditionally, jurisprudence considered signing to mean directly placing one's name on a paper medium by hand in one's own handwriting[7]. It is automatically assumed that a paper document signed by hand fulfils the three previously listed functions (identification, integrity and appropriation).

The handwritten signature is a unique means of identification that is linked to only one particular person. A layman can compare different signatures from one person and can form an accurate impression about the authenticity of the signature without requiring special resources. In cases of doubt, a graphologist can provide a definitive answer on the authenticity of a signature, as he can determine with near certainty whether the handwriting belongs to a particular person.

It is sufficiently difficult to manipulate a paper document, by changing content, adding or deleting information, in a way that will not be noticed. Paper is therefore a prime medium to record information in an unchangeable way.

Legal custom has it that by placing his signature, the signatory expresses his agreement with the content of the document.

This view of the handwritten signature also explains the difference between original documentary evidence and a copy of it. Only the document bearing the original signature is an original with the corresponding special evidential value. The law of evidence considers a document on which the signature appears in another form, for instance by using scanning techniques or microfilm, to be a "copy" and not an original.

The law of evidence attributes greater value to an original document than to a copy of this document. Article 1334 of the Belgian Civil Code stipulates that a copy will only be accepted as evidence when the original can still be produced. The opposing party can thus always challenge a copy and demand the submission of the original. This is very important when documentary evidence on paper is included in a digital archive (e.g. via scanning techniques). Usually the original is destroyed and can no longer be submitted. The electronic version is only a copy because it lacks a valid signature and thus has only limited evidential value. However, as long as the opposing party does not challenge the copy, the copy does have the same cogency as the original. The court may not demand the submission of the original if none of the parties does so.[8]

3. THE ELECTRONIC SIGNATURE

Until recently, the rules governing documentary evidence impeded the proof of agreements entered into electronically. The enforceability of these contracts in court was subject to great legal uncertainty, as such agreements could obviously not be signed by hand.

Printing contracts concluded electronically could not provide a satisfactory solution. After all, the printout is a document that lacks an original signature and thus can at best be considered only a copy.

The incompatibility of the rules of evidence in the Belgian Civil Code with modern information and communication technologies was a considerable impediment to the use of the information highway for legally relevant acts[9].

Since 1 January 2001, new rules on the admission of electronic signatures have gone some way toward alleviating these problems. A digital document can now, in principle, fulfill the requirements of a signed document as the electronic signature is now equivalent to a manual signature in the eyes of the law.

3.1. THE ELECTRONIC SIGNATURES ACT AND CERTIFICATION SERVICE PROVIDER ACT

At the end of the 1990s various European member states started adapting their rules of evidence to modern technologies. There was a fear that differing rules for the legal recognition of electronic signatures would arise within the European internal market. This could present serious obstacles for the development of electronic trade. That is why a directive was issued to create a common framework for electronic signatures on a European level[10]. The Electronic Signatures Act[11] and the Certification Services Provider Act[12] incorporated the European framework in Belgian legislation.

An electronic signature is any electronic substitute for the traditional handwritten signature. A frequently used technique in many electronic document management systems for creating electronic signatures is the "digitized handwritten signature". The signer copies the digital, graphical representation of his own signature (bitmap) to the word processing file that contains the document he wishes to sign. The bitmap is created by scanning the signature. The users of this system use a password to gain access to their own signature.

This tecnique captures the look and feel of a handwritten signature and this type of electronic signature will thus be easily recognized as a signature by layman. There are many other techniques besides this for creating an electronic signature. At present, the "digital signature" technique is the most advanced technique[13]. In contrast to the digitized handwritten signature, the digital signature does not resemble the handwritten signature at all[14].

Since 1 January 2001, an electronic signature can also be considered a valid signature[15]. Electronic data can constitute a valid signature subject to two conditions:

- It must be possible to attribute the electronic data that constitute the signature to a particular person (the signature's identification and appropriation functions)
- The electronic data that constitute the signature must demonstrate the preservation of the document's integrity (integrity verification)

When the electronic signature satisfies these two conditions, the judge will accept it as a valid signature. If he ascertains that one or both conditions are not satisfied, then he will not accept the digital document submitted to him as a signed document, but as a normal document the credibility of which he may evaluate himself.

The contracting parties are accorded the freedom to choose from numerous techniques to sign their documents. The court may not ignore documentary evidence that is signed with an electronic signature solely because the signature is placed in electronic form[16]. From now on, a digital document with an electronic signature is admissible evidence, regardless whether the two conditions explained above are fulfilled.

In the European context, considerable differences in interpretation could arise between member states with regard to which signature techniques are acceptable. To correct this, the directive has defined one type of electronic signature that must be accepted everywhere in the European Union as the equivalent of the handwritten signature. This type of signature is called a "qualified electronic signature".

3.2. QUALIFIED ELECTRONIC SIGNATURES

A description of a qualified electronic signature can be found in the Certification Services Provider Act. It is an "*advanced electronic signature*, based on a *qualified certificate* and created by a *secure signature creation device*"[17]. Each of these three elements requires a word of explanation.

A qualified signature is first and foremost based on a technology that produces advanced electronic signatures. A signature is called *advanced* when it:

- is linked to the signatory in a unique way
- it is capable of identifying the signatory
- it is created through means that the signatory can keep under his exclusive control
- is linked to the data on which it is based in such a way that any subsequent change to the data can be detected.

With currently availble technology, only the digital signature technique is suitable to create advanced electronic signatures. In the future, other techniques that satisfy these conditions will probably be developed.

Next, a qualified signature is accompanied by a qualified certificate. A certificate is qualified when it contains a certain set of information[18]:

- the label "qualified certificate";
- contact information of the certification authority (CA);
- the certificate holder's name or pseudonym;
- the period of validity;
- signature verification data corresponding to the signature creation data held by the certificate holder;
- the certificate's identity code;
- the advanced electronic signature of the issuer of the certificate.

Where appropriate, the following information can be added:

- reference to a specific attribute of the signatory, for instance his profession;
- the restrictions on the use of the certificate;
- the limits relating to the value of the transactions for which the certificate may be used.

Certification authorities that wish to provide such qualified certificates must satisfy several conditions:

- they must demonstrate that they are sufficiently reliable to supply certification services;
- they must ensure the operation of a prompt and secure directory service and of an immediate revocation service;
- they must see to it that the date and time when a certificate is issued or revoked can be determined accurately;
- they must use reasonable means to verify the identity and, where applicable, the specific attributes of the person to whom a qualified certificate is delivered;
- they must employ personnel with the specific knowledge, experience and qualifications necessary to provide the services and, in particular competence at managerial level, expertise in electronic signature techology and familiarity with proper security procedures; they must also apply administrative and management procedures and methods adapted to and consistent with the recognized standards;
- they must use trustworthy systems and products, which are protected against modification and which guarantee the technical and cryptographic security of the processes that they support;
- they must take measures against the forgery of certificates and when the certificate-service provider generates signature creation data, they must guarantee the confidentiality of that process;
- they must have sufficient financial resources to operate in accordance with the requirement of this Act and in particular to accept liability for damage, for instance, by taking out suitable insurance;
- they must record all relevant information about a qualified certificate during the useful period of thirty years and, in particular, be able to submit proof of certification during legal proceedings. These records may be stored electronically;
- they must neither record nor copy the data for creating the signature of the person to whom the certification-service provider has granted key-management services;

- they must notify every applicant for a certificate via a durable means of communication about the exact modalities and conditions for using the certificates, including the imposed limitations for their use, about the existence of a voluntary accreditation system and about the procedures for complaints and the settlement of disputes. This information, which can be transmitted electronically, must be in writing and formulated in language that is easy to understand. Upon request, relevant elements of this information must also be made available to third parties who rely on the certificate;
- they must use trustworthy systems to store the certificate in verifiable form so that:
    a) only authorized persons can enter and modify data;
    b) the authenticity of the information can be verified;
    c) the certificates will only become publicly available in the cases in which the certificate holder has granted his permission and
    d) the user must clearly understand each technical modification that poses a risk to security requirements.

Most of these conditions are rather vaguely formulated so it remains to be seen how they will be interpreted in practice. Certification authorities can request accreditation voluntarily from the Federal Public Service for Economy, SME's, Self-Employed and Energy[19]. This accreditation will serve as a quality label for certification authorities that satisfy the requirements in annex 2, that provide certificates that comply with the requirements in annex1 and that use means to create signatures that comply with the requirements in annex 3 of the Certification Services Provider Act.

Finally, a qualified signature is created using a secure signature creation device, as is described in annex 3 to the Certification Services Provider Act:

- The information used to create a signature must be unique and non-recurrent. Everything possible must be done to ensure the confidentiality of this information.
- The certificate holder must have reasonable certainty that information used to create the signature cannot be derived from the resulting signature or the certificate. The signature should be protected against forgery using currently available technology.
- The certificate holder must be able to protect the data for creating the signature reliably against use by others.

The qualified electronic signature is not the only legally valid electronic substitute for the handwritten signature. The only advantage that this type of signature has when compared to other electronic signatures is that it is automatically recognized as the equivalent to a handwritten signature everywhere in the EU. As soon as a judge has pronounced an electronic signature qualified, he is obliged to consider the document that bears it to be validly signed. Consequently he will automatically accept the digital document submitted to him as a signed document.

3.3. SCOPE OF THE NEW REGULATIONS

The introduction of the electronic signature into the law of evidence is only a small step in the modernization of our law. Contracts can now be drafted and signed electronically. If all conditions have been fulfilled, such an electronic contract will have the special evidential value of a privately signed document.

But this does not mean that an electronic signature can always replace a handwritten version. It is not yet possible to apply to city hall for a building permit or take out a mortgage electronically. The signature is not required here as evidence, but for the validity of these transactions. In certain cases, other formal conditions besides the signature exclude electronic documents. For instance, a unilateral promissory note must contain the handwritten phrase "read and approved".

These gaps will gradually be filled in the future. The Electronic Commerce Act, which will be covered later on, has gone part way in this direction.

4. EXCEPTIONS TO THE SIGNED-DOCUMENT REQUIREMENT: UNREGULATED EVIDENCE SYSTEM

For some activities, the law does not require that an original signed document be drafted as evidence. In these cases, the parties may submit any and all types of evidence to the court. The conditions that apply to the electronic signature need not be taken into account in these cases. For instance, unsigned e-mail messages are admissible as evidence.

4.1. COMMENCEMENT OF WRITTEN PROOF

The lack of a proper documentary evidence, namely an original signed document, is excusable when one submits other reliable evidence in written form. This mode of proof is called a commencement of written proof in legal jargon. The term "written" must be interpreted broadly: it can mean an irregular authentic act that doesn't comply with all required formalities to be valid, a simple letter, a fax, or even an electronic document. However, only documents originating from the party against whom they are used qualify. A document originates from someone when he created it or appropriated it as his own[20]. An item of evidence that one creates oneself is just not as convincing. As the term "commencement of proof" suggests, additional supporting evidence is still necessary, such as circumstantial evidence or witnesses. This in contrast to the special evidential value awarded to original signed documents.

4.2. TRANSACTIONS WITH A LIMITED VALUE

Any type of evidence can be used to substantiate transactions with a value of less than 375 EUR. When someone uses internet to order books or CDs for a value that does not exceed 375 EUR, no electronically signed document is required. A regular e-mail is sufficient. However, in these cases the court may decide upon the credibility of the e-mail (or of other electronic data). A plain document does not have the special evidential value of a signed document.

Under these circumstances the original paper documents (whether signed or not), which were drafted when entering into the agreement, may be replaced by an electronic scan for the purposes of archiving sufficient evidence of these relatively unimportant agreements.

4.3. FORCE MAJEURE OR "ACT OF GOD"

Similarly, it is not necessary to submit proper documentary evidence when the creditor was unable to procure written evidence due to force majeure or an "act of God" (art. 1348 of the Belgian Civil Code). In some situations, circumstances beyond one's control prevent the drafting of a document. In other cases, documentary evidence that had been drafted is lost due to an unforeseen accident caused by circumstances beyond one's control. Evidently, purposely destroying the original evidence to replace it with electronic images does not fall within the scope of this exception.

4.4. COMMERCIAL EVIDENCE LAW

The rules of evidence in commercial law are traditionally more flexible than the civil rules of evidence. Businesses may use any and all types of evidence to substantiate their assertions. The judge determines the credibility of the evidence presented as he sees fit. This unregulated evidence system is based on art. 25 of the Belgian Commercial Code.

In principle, a signed document is never required as evidence between businesses, regardless of whether the value of the transaction exceeds the 375 EUR limit. Contrary to civil law, in business there is no incentive to draft signed documents as commercial law does not attribute any special evidential value to such proof. The judge determines the credibility all submitted proof, electronic or otherwise. This arrangement is prompted by the rapid and informal character of business transactions.

Under these circumstances original paper documents may be replaced by electronic data, e.g. using scanning techniques or microfilm, for archival purposes.

The scope of the commercial rules of evidence is very narrow: only business to business relations are concerned. When one of the parties is a private individual, then the civil rules of evidence apply when a dispute arises. The business partner must thus be able to submit a signed document for transactions having a value in excess of 375 EUR. If the transaction is concluded through electronic means, both parties must place an electronic signature on the electronic document. The private party, by contrast, may apply the more flexible rules of commercial law when submitting evidence against a business.

Moreover, businesses are often obliged to store information in paper form for reasons other than the law of evidence. The government exercises control over businesses for economic, social security, tax and other purposes. The way in which this inspection is organized still frequently implies the use of paper documents, handwritten signatures, etc., which impedes an efficient use of electronic information and communication technology[21].

5. EVIDENCE LAW TAILORED TO THE INFORMATION SOCIETY

The introduction of the electronic signature into Belgian law has prepared the rules of evidence for the information society. The private contract, the prime example of documentary evidence, can now also be drafted and signed electronically. The parties to a contract are free to use a variety of techniques to sign their documents as long as the attribution and integrity of the signature is guaranteed. The fulfillment of these conditions will be verified by the judge in case of a dispute. The use of a qualified signature is by no means mandatory, but such a signature has the advantage that it is valid throughout the European Union as a substitute for a handwritten signature.

The modernization of evidence law is nevertheless only one step in a broader development. In some cases, a signature is a formal condition for validity, for instance on an authentic act. Beside this there are still other formal requirements for the validity of many types of documents, for instance inclusion of a handwritten notice or the use of a watermark. These legal obstacles are gradually being removed. The Electronic Commerce Act has already removed several obstacles, as has the Electronic Invoice Act. Other measures will follow in the future.

E. THE ELECTRONIC COMMERCE ACT

In the wake of the directive issued by the European Union[22], Belgium enacted the Electronic Commerce Act[23]. The intention of this law is to create a favorable framework for the development of electronic commerce. In addition to measures to strengthen consumer confidence and to limit the liability of certain intermediaries in the information society, it also tackled the remaining obstacles for online contracts.

The Act's scope is limited to "services of the information society" (art. 3 of the Electronic Commerce Act). This is defined as any service, normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services (art. 2 1° of the Electronic Commerce Act)[24]. "Normally provided for remuneration" means as part of an economic activity. Occasional rendering of services electronically also falls under this heading; the term "usually" concerns the remuneration and not the use of electronic means[25].

Certain services do not fall under the application of the law, specifically the official activities of civil law notaries, the representation of clients by attorneys and gambling (art. 3 4° of the Electronic Commerce Act).

1. ONLINE CONTRACTING

The intention of the Electronic Commerce Act is to remove all obstacles that hinder entering into contracts in relation to a service of the information society. All steps in the process of contract conclusion are addressed, from the initial negotiations, over the tender, the signing, the invoicing to the registration and archiving of the contract. The current requirements of form are not abolished, but it will be possible to fulfill them electronically.

Next to the signature, our law contains other formal prescriptions that hinder the conclusion of contracts electronically. Besides several direct obstacles, such as the formal obligation to use paper, there are also many indirect obstacles. Uncertainty exists concerning the application of some procedural requirements on contracts entered into electronically. A few examples are "registered mail sent by the postal services"[26], inclusion of handwritten notices, drafting multiple copies, use of special layout or forms, etc. Frequently, these formal requirements must be satisfied to ensure the validity of the contracts or other legal transactions involved, and not only to constitute evidence, as described in the previous chapter.

The legislator chose not to tackle existing procedural requirements one by one, because such a comprehensive analysis of Belgian law would be too time consuming. Instead several transversal stipulations were introduced that cut across the entire body of law. In the past, this method was used to introduce the euro into Belgian law.

Art. 16 §1 of the law stipulates that any legal or regulatory requirement of form applicable to the conclusion of contracts is deemed satisfied if the functional qualities of this requirement are fulfilled. In other words, the parties to the contract may develop their own electronic alternative for existing formal requirements. Thus, it is necessary to determine the objective or functional qualities of each formal requirement. This is not a simple task, since most formal requirements do not state the objective they pursue. Similar requirements of form can pursue different objectives depending on the legislation that imposes them. For instance a signature is sometimes required as evidence and sometimes for the validity of a legal transaction. The contracting parties will only be absolutely certain that the electronic alternative they developed suffices when a judge has confirmed this in the event of a dispute.

Art. 16 §2 provides further information regarding formalities that are very common. This is the case for the writing, the signature and the handwritten notice. Nonetheless, the parties to the contract must perform the same exercise for these three procedural requirements as for any other procedural requirement. Under certain circumstances a writing, a signature or a handwritten notice can have other functional qualities than those explicitely described in the Electronic Commerce Act.

A writing is a series of legible signs that must be accessible for later consultation whatever the medium and modalities of transmission may be. Thus "writing" may no longer be equated with a paper document. Electronic information stored on diskette, CD-R, CD-RW, DVD, chip card and the like constitute a writing insofar as the content can be made legible for people with the aid of a computer and suitable software. Moreover, the medium must also be sufficiently durable to allow the information stored to be accessible for later consultation.

Regarding the signature, we are referred to the rules on the electronic signature in the Belgian Civil Code and the Certification Service Provider Act. The requirement of a signature is fulfilled when the electronic signature satisfies the two conditions set by the evidence rules (identification and integrity) or when the electronic signature is a qualified electronic signature (presumption that these two conditions have been fulfilled).

At first glance, it is strange to see a reference here to already existing regulations governing the electronic signature. The reason is to provide legal recognition beyond the scope of evidence law. Whereas the Belgian Civil Code and the Certification Services Provider Act do not affect the legal status of the electronic signature outside the rules of evidence, the Electronic Commerce Act recognizes the electronic signature for use in all aspects of the contractual process. From now on, whenever a signature is required in any stage of contract conclusion, an electronic signature is a valid alternative. This is important, for instance, when a signature is needed for the validity of a contract[27].

Nevertheless, one must bear in mind the limited scope of the law: if affects only formal requirements that must be fulfilled in the conclusion of a *contract*. For the time being, obstacles for transactions that are not contracts may continue to exist. A contract always presupposes two parties. A legal transaction in which there is only one party is not a contract but a unilateral legal act. One example of this is the unilateral promissory note, which requires a signature to be valid.

Finally, the law offers an electronic equivalent for the requirement of a handwritten notice. This requirement can be satisfied electronically by using a procedure that guarantees that the notice genuinely originates from the supposed author. With current technology, the digital signature appears the most appropriate technology to achieve this.

For some formal requirements finding a functional equivalent is impossible. For instance, an electronic contract cannot be registered with the registrar of mortgages because this requires a date stamp, which to date still means applying a physical stamp onto a paper document. In such cases the King may elaborate an alternative in a Royal Decree (art 16 §3).

A specific stipulation concerning registered mail, in some cases "registered mail sent by the postal services", was not deemed necessary. Since the Royal Decree of 9 June 1999[28], the requirement of registered mail no longer poses a legal obstacle for concluding contracts electronically. This Royal Decree stipulates registered mail can take any appropriate form, amongst which paper or electronic form. A subsidiary of the Belgian Postal Service offers a service for registered e-mail[29]. Nevertheless, there is no obligation to use the services of the Belgian Postal Service, even when the law speaks of a "registered mail sent by the postal services". Today, several companies offer services to send e-mail with receipts. Use of the Belgian Postal Service for registered mail is obligatory in only one case, namely when the registered letter is used in legal or administrative proceedings.

2. EXCEPTIONS

The law does not alter the formal requirements that impede the conclusion of contracts electronically for certain types of contracts. These exclusions will remain until the legislator expressly abolishes them. The following types of contracts are involved:

- The transfer of property rights on real estate, in whole or in part.
- Contracts that fall within the scope of family or inheritance law, for instance nuptual agreements.
- Contracts that must be concluded before a civil law notary or a public official, such as an authentic act.
- Contracts of suretyship granted and on collateral securities furnished by persons acting for purposes outside their trade, business or profession.

The formalities proscribed in these cases cannot be replaced with a simple set of transversal stipulations. The law imposes several special guarantees for these contracts, such as the intervention of a third party, the drafting of an inventory, the presence of witnesses, etc. In the coming years, the legislator must examine how these guarantees can be maintained in an electronic environment. Until then, these agreements must be recorded on paper.

The Electronic Commerce Act takes a carefull first step in this evolution by stipulating that an authentic act may be drafted in electronic form and that the the public official may sign electronically.[30] However, the practical implementation of article 31 is subject to a royal decree being discussed in the council of ministers[31]. The authentic act is primarily known as a document drafted by a civil law notary, but it can also be drafted by other public officials (a judge, a mayor or a registrar of births, deaths and marriages). To be authentic, the document in question must be drafted by the competent public official in the manner prescribed by law[32]. Authentic acts must typically be archived for very long periods of time, some must be kept indefinitely. It is not yet clear how this can be achieved with electronic documents. Because of the major importance of these acts, this matter will not be treated lightly and the first electronic authentic act is presumably still a long way off.

3. COMMERCIAL LAW AT TWO SPEEDS

The Electronic Commerce Act removes several of the remaining legal obstacles to concluding contracts electronically. The parties to the contract are granted a great amount of freedom to develop their own electronic alternatives for the formal requirements that were created for the paper world. This freedom comes a the cost of a greater degree of uncertainty concerning the legal validity of the procedures they have developed. In time this problem will become smaller as jurisprudence demarcates what is acceptable from what is not.

Important to keep in mind is that this freedom is only granted for commercial transactions related to a service of the information society. As a consequence businesses must create parallel systems: one for online contracts concluded as part of a service of the information society and another for all other commercial transactions. Each transaction must be situated in the correct category so that the necessary items of evidence and documents can be drafted in the correct form. The legal uncertainty that this entails is detrimental to the further automation of commerce.

F. BOOKKEEPING AND ANNUAL ACCOUNTS

Besides the conclusion of contracts with customers and trading partners, many internal operational processes within companies are suitable for automation.

Accounting, invoicing and the submission of the annual accounts are but a few examples of such processes. Nevertheless, the law still imposes important limitations in this domain. The administration is still largely oriented toward a paper accounting system, from the perspective of accounting law as well as from that of tax law. Modernization of the legislation is more advanced when it comes to invoicing and submitting annual accounts.

1. ACCOUNTING OBLIGATIONS

The purpose of keeping accounts is to provide the company and third parties with a realistic and complete picture of the company's assets, financial situation and results. In Belgian law, the Accounting Act[33] and its executory decrees form the regulatory framework for accountancy.

The Accounting Act is nearly thirty years old and was written when a paper accounting system was self-evident. The law has not evolved with the technological developments, which have led to wide-scale use of automated bookkeeping systems by companies both small and large. Today, the native form of the bookkeeping is almost exclusively electronic. Because of the accounting regulations some of the books must still be printed on paper because certain formalities can only be fulfilled in paper form.

In compliance with art. 5 of the Accounting Decree[34], the most important ledgers must be stamped by the clerk of the commercial court holding the trade register where the company is located. The law lists the ledgers concerned, specifically the cash received ledger, the central ledger and the inventory ledger. The company may keep bound registers made in accordance with an approved model. If a company works with loose sheets, the clerk must also put a stamp or sign his initials on each sheet. From the wording of the Accounting Decree, it appears that it is presupposed that the ledgers are kept manually on paper. For this reason, only the paper version of these ledgers is considered legally valid.

Other parts of the accounting books, such as the subsidiary journal, need not be stamped or signed and may thus be kept "on any other suitable material". An electronic version can also be legally valid[35]. A condition for this is compliance with the general accounting principles, set out in article 7 §2 of the Accounting Act. More specifically there must be certainty that the entries cannot be modified once entered. This principle applies to both traditional, manual bookkeeping systems as to automated bookkeeping systems.

Accounting software or systems must be designed in such a manner that a definitive entry can only be changed by a counter entry. The original entry must also always remain visible[36]. In practice however, many accounting applications disregard this fundamental rule of accounting. Strictly speaking, this implies that even the unstamped ledgers must also be recorded in "directly legible documents" in order to comply with the law.[37] A "directly legible document" means a paper document.

The Accounting Act is more flexible when it comes to documents that provide evidence supporting the books. These documents may be exchanged in electronic form, again on the condition that the information they contain cannot be modified once it has been finalized.

The ledgers must be stored for ten years starting from the first of January of the year following that in which they were closed[38]. This long retention period imposes a heavy burden on companies, as physical storage space is usually quite costly. To accommodate this the legislator allows the unstamped ledgers to be kept either in the original form (on paper or electronically) or as copies. The original unstamped paper ledgers, where applicable, may then be destroyed. The stamped books, by contrast, must still be stored in the original paper version.

The supporting documents must also be stored for ten years. This period is reduced to three years when they cannot serve as evidence vis-à-vis third parties. These documents may be stored in original form (on paper or electronically) or as copies[39]. The original paper accounting documents may be scanned and stored in digital form. The paper original may then be destroyed.

2. ACCOUNTING AND TAX LAW

Beside the economic inspection authority, the tax authorities also have an interest in the accounts. The legislation on income tax and the VAT regulations both impose obligations regarding maintaining and preserving books. Sometimes these rules diverge from those of accounting law. As far as income tax is concerned, the taxpayer is obliged to store all ledgers and records that can be used to determine the amount of taxable income. The tax authorities can demand this information up to the end of the fifth year (according to the civil calendar or the accounting calendar) following upon the taxable year[40]. For the VAT, art. 60 of the VAT Act sets the storage period for ledgers and records at ten years.

Traditionally tax law adopts a rather more pragmatic attitude than does accounting law. The tax authorities sole aim is an accurate tax levy, which results in a less formalistic approach: the content of the accounts is more important than their form. There is no question of a stringent regulation of the form which the accounts must take. An accounting system that does not comply with all the formalities of accounting law can still have evidential value for tax purposes.

The tax payer must be able to present to the revenue service the mandatory ledgers and documents, such as the receipt books required by article 320 of the Income Tax Code, the documents that have served for keeping accounts and in general all documents that can be useful in determining the taxable base. For the VAT purposes, the accounts consist of the following ledgers: a ledger for incoming invoices, a ledger for outgoing invoices and a journal in which receipts are recorded for actions that are exempt from the obligation to draft an invoice[41].

To exclude any possibility of doubt, the tax legislation was modified to allow automated bookkeeping and electronic supporting documents[42]. However, the tax authorities also apply the principle that accounting entries may not be modified once finalized. So the integrity of the stored information must be ensured throughout the retention period.

Moreover, the tax authorities retain the right to demand that the ledgers and records be presented in a legible and comprehensible form[43]. The tax officials may demand copies of electronic ledgers and records in a form of their choice. Finally, they can request the taxpayer to repeat his calculations to ensure that the correct tax is levied. This last obligation has far-reaching consequences. The bookkeeping must not only be preserved, it must be preserved in such a way that calculations can be performed with the data. This obligation entails a considerable extra cost for companies that keep their accounts electronically. The company can opt to preserve the computer system in which the books and records were created in operational condition[44]. However, maintaining an obsolete computer system for a long period is far from obvious. The cost of maintenance and replacement parts can be high. Moreover, in some cases the company will have replaced its accounting system more than once during the mandatory retention period. A second option is to migrate all the accounts to the new accounting system, provided that there are sufficient guarantees that the books will remain unaltered.

As is the case in accountancy law, the regulation on income tax and VAT requires, in principle, that all original paper documents be preserved. As an exception, the income tax and VAT authorities allow certain ledgers and records to be stored on microfilm, micro cards or CD-WORM[45].

The ledgers and records involved include the following:

- The duplicates of documents drafted by the taxpayer and correspondence that was not supplemented or signed by the addressee, with the exception of any documents bearing an official seal or any other mark required by tax regulations. The copies of outgoing invoices may be scanned then destroyed. Original purchase invoices, bank statements, receipts and duplicates of VAT slips that restaurants are required to provide to their customers are excluded from this regulation. Any document to which an invoice refers for the description of the delivered goods or services, such as the tender documents and shipping note must be preserved under the same conditions as the incoming invoice.
- The ledgers and registers prescribed by the VAT Act, with the exception of the receipts journal. The ledger for incoming invoices and the ledger for outgoing invoices may also not be replaced by microfilm or micro cards for retention purposes when they are among the ledgers stamped in accordance with the Accounting Act[46].
- Documents supporting the books such as the general ledger accounts.

The conditions for storage on microfilm or micro card are the same for both income tax and VAT. The most important are:

- Outgoing invoices must be stored on film, card or CD-WORM in the order of their registration in the outgoing invoice ledger. The other documents must be stored in chronological or numerical order.
- Each film, card or CD-WORM may only contain one book or one particular type of document.
- The films, cards or CD-WORMs must be presented to the tax officials upon request. The taxpayer must be able to show the documents on a screen and allow copies to be made of them, without moving the documents.
- When an automated bookkeeping system is used, the data must be written to a CD-WORM on a daily basis.
- No prior authorization is needed before using this preservation method, but the taxpayer should provide the authorities with some information in advance, such as what type of material will be used.

Although this solves a part of the storage problem, the scope of this exemption is limited. The requirement to preserve the originals still remains for many items of evidence. Moreover, the solutions offered aren't very flexible, as the administration only accepts certain technologies. The technological evolution has not slowed its pace and the CD-WORM is gradually becoming obsolete due to the rise of the DVD-WORM and software-based WORM solutions. Finally, this exemption only applies in relation to the tax authorities, while the rules of evidence vis-à-vis third parties are not affected.

3. ELECTRONIC INVOICE

The invoice is one of the most important items of evidence in accounting. Strangely enough, no definition of this concept can be found anywhere in the legislation. First and foremostly an invoice is a commercial document that summarizes the content of a contractual obligation and invites the customer to pay. In addition the invoice plays an essential role in the VAT system. The tax authorities use the information invoice to assess the amount of VAT owed by taxable persons. For this reason the legislator has imposed an invoicing obligation on suppliers of goods and services[47]. Only the person holding a complient invoice may deduct VAT already paid from what they owe the tax administration.

The technology to exchange invoices electronically has been around for several years. Companies are very interested in the savings this could bring, and the tax authorities are also gradually coming to discover numerous advantages to the electronic invoice. Research has shown that the cost of a paper invoice lies somewhere between 1.13 EUR and 1.65 EUR, against 0.28 EUR to 0.47 EUR for an e-invoice[48]. Electronic invoicing is a logical step in the increasing automation of business processes.

Until recently the lack of a uniform framework in the European Union hindered the breakthrough of electronic invoicing. Large companies and specialized service providers did not succeed in drafting uniform invoices that satisfied the conditions of all Member States. Such centralization would help keep down the administrative expenses borne by European companies and consequently could strengthen their competitive position with respect to business from third-party countries. The European Union issued Directive 2001/115 on the harmonization of invoicing regulations[49] to eliminate these and other invoicing bottlenecks. In addition laying down common rules governing self-billing and the out-sourcing of billing operations, this directive creates a uniform legal framework for electronic invoicing and electronic preservation of invoices. The law of 28 January 2004 (*Moniteur belge*, 10 February 2004) incorporated this directive into Belgian law.

Various e-invoicing platforms have been available on the market for several years. There are two basic types of systems: invoicing via EDI platforms and invoicing via e-mail. EDI (Electronic Data Interchange) implies that the trading partners exchange messages automatically between their computers without human intervention. For this purpose, messages are structured according to a previously agreed standard. E-mail invoicing can be automatic as well as manual. The invoice can be sent as attachment, but all the information necessary for an invoice to be valid can be present in the body of the e-mail. To allow automatic processing, the information can be structured, for instance by using XML.

In principle, the supplier of goods or services is obliged to draft an invoice for every delivery that he makes. He can also opt to mandate his customer or a third party to draft the invoice in his name[50]. Even though the concept "invoice" was not defined in the Belgian VAT Act, the tax authorities used to presuppose that an invoice was necessarily a paper document. Exceptionally the tax authorities granted certain companies a license to invoice electronically. Since 1 January 2004 electronic invoicing is open to everyone, insofar as the legal conditions are respected. First of all, the other party to the contract must be willing to accept an electronic invoice. This acceptance can be expressed explicitly or implicitly[51]. In addition, the authenticity of the invoice's origin and the integrity of its content of must be guaranteed. To achieve this the person issuing the invoice can use two techniques, either he signs the invoice with a secure electronic signature, or he sends the invoice in accordance with the "EDI-standard code"[52].

The concept "secure electronic signature" is synonymous for the advanced electronic signature referred to in the Certification Services Provider Act[53]. A qualified certificate is not required. Although the term "signature" is used, this is not a signature in the legal sense. After all, the Directive states that the Member States may not ask that the invoice be signed[54]. In this context the concept "secure electronic signature" refers exclusively to the technical notion. The term "electronic stamp" would perhaps have been more suitable.

The concept "EDI-standard code" does not refer to an official EDI standard, such as UN/EDIFACT, but to the message structure to which the parties have agreed[55]. In each case the EDI procedures that have been agreed upon must guarantee the authenticity of the origin of the invoice and the integrity of the data.

In principle a simple e-mail does not suffice as a valid invoice. Nevertheless, the Ministry of Finance has the right to accept a normal e-mail and even other methods of electronic invoicing insofar as the authenticity and integrity are guaranteed. Systems that use unsigned e-mail messages and rely on an audit trail to guarantee the authenticity and integrity of individual invoices could be legalized in this manner[56].

The directive forbids Member States from imposing more stringent conditions, except for invoices originating in a country outside the EU for goods and services delivered in Belgium.

An invoice must always be drafted in duplicate[57]. The original copy is intended for the customer, while the person registered for VAT must store a copy. Article 60 of the Belgian VAT Act imposes the obligation on both the person registered for VAT and the customer to preserve invoices for ten years. Nevertheless, the authorities accept that the customer – when a natural person purchasing goods or services intended for private use and to whom an invoice was still delivered – must only store the invoice for five years.

Paper invoices must be stored in Belgium, thus ensuring easy access for inspection by the tax authorities. The same requirement applies to electronic invoices in principle, allthough these may be stored anywhere in the EU if the taxpayer notifies the authorities about this in advance[58]. In this case the authorities must receive online access to the invoices stored in another Member State (art. 61, §1, par. 3 of the Belgian VAT Act). Storage in outside the EU is totally excluded, allthough the directive stipulates that this should be allowed when there are administrative agreements with the non-member country in question[59].

The customer must store his original invoice in the form in which it was received, be it on paper or electronically[60]. He can only exercise his right to deduct VAT paid when he can submit an original invoice. The supplier may preserve his copy of the paper invoice on microfilm, micro card or CD-WORM and destroy the paper copy.

The authenticity of the origin and the integrity of the content of the invoice as well as its legibility must be guaranteed throughout the entire retention period. Moreover, the information that guarantees the authenticity and the integrity of the electronic invoice must also be preserved[61].

The new legal stipulations give companies greater freedom to adapt their invoicing procedure to their needs. The law limits itself to establishing the objectives that an invoice must meet and is formulated in a technologically neutral manner. This procedure must largely protect the legislative framework from obsolesce due to the rapid evolution in technology. Unfortunately, the executory decrees restrict the freedom offered again to a great degree. As such, both EDI and the secure signature allow a broad scale of implementations, yet several other procedures are excluded *a priori*. It is to be hoped that the Finance Minister will remove these restrictions again in the near future.

4. PUBLICATION OF THE ANNUAL FINANCIAL STATEMENT

In addition to maintaining regular accounts, companies must submit an annual financial statement each year to the National Bank of Belgium (NBB)[62]. This statement must include a statement of assets and liabilities, a statement of earnings and the notes to the financial statements. For financial statements drafted integrally in accordance with either the full scheme or the abbreviated scheme[63], the submitter may choose to transmit the documents in an electronic form, either by handing over a diskette or via the internet, or may choose to submit them on paper[64].

Exceptionally the annual financial statement must still be presented on paper when it is drafted in a currency other than the euro[65] or when some headings in the statement were adapted to the special nature of the company's activities.

The Central Balance Sheet Office publishes the technical specifications that financial statements submitted on diskette must satisfy in the "*Protocol* for Submitting Annual Financial Statements on Diskette"[66]. Various companies use this *protocol* when developing software to draft annual financial statements. Alternatively, the person required to submit the statement can download a free submission program from the National Bank of Belgium.

Submission through the internet is not yet available to all companies. For the time being companies must obtain prior approval from the National Bank of Belgium. In January 2004, the NBB launched a pilot project for submitting annual financial statements over internet. Only third-party submitters who submit many financial statements for their customers may participate in the pilot project. It is hoped that this system will be opened to all standardized financial statements[67] in the course of 2005.

The company must already have performed the arithmetic and logical verification of the annual financial statement before submitting it in electronic form. The National Bank examines the annual financial statements submitted on paper. Each annual financial statement must be placed on a separate diskette or in a separate electronic message[68]. The lower fee that applies to electronic submission is intended to stimulate its uptake[69].

5. PAPER LOSES GROUND

The accounts and the annual financial statement derived from them play an important role in the amount of control exercised over companies by creditors, shareholders and by the government. From a legal perspective, switching to electronic accounting entirely remains out of reach; nevertheless, paper accounting is losing ground. Certain documents may be created electronically from the start, while others may be converted from paper to electronic form. It is only mandatory to draft and store core accounts on paper.

The annual financial statement may be submitted electronically, insofar as this does not diverge from the prescribed standards. For the time being, only submission on diskette is open to all companies, but in the future submission over internet will be open to everyone.

Greatest progress occurred in the area of invoicing. Prompted by the European Union, all Member States developed a similar legal framework for the exchange of electronic invoices.

G. SOCIAL DOCUMENTS

1. WHAT ARE SOCIAL DOCUMENTS

Already in 1896 employers were required to maintain a personnel register. Today, the regulations governing social documents can be found in Royal Decree no 5 of 23 October 1978 on the keeping of social documents (*Moniteur belge*, 2 December 1978). This Royal Decree lists the social documents:

- the general and special personnel registers
- the individual account
- the attendance register
- the written employment contracts for the employment of students and domestic servants,
- the apprentice contract for part-time pupils
- documents relating to the employment of special categories of employees

The law requires all employers to maintain social documents so that it can be determined at any moment which employees work for a given employer. The objective is to facilitate exercise of control by the social inspection authority on illegal workers.

The personnel register is a register in which all employees are registered in chronological order of the commencement of their employment. In principle, the employer must maintain one personnel register for all his employees. Separate registers for white-collar and blue-collar workers are not allowed[70]. The special register is only required when the employer has people working at more than one location. In this case, a separate personnel register is kept at each location[71].

The individual account is a detailed description of the work an employee has performed for his employer during a given year. It also states the days worked, the days not worked, the elements that make up the salary and the deductions from it (social security, income tax, etc). The individual account also contains all useful administrative information in relation to the salary (for instance, the joint committee, the employer's salary administration service)[72].

The law of 3 July 1978 (Employment Contract Act) obliges the employer who hires a student or home worker to draft a written employment contract containing several mandatory clauses. An analogous obligation applies to an apprentice contract for part-time pupils[73]. These documents serve as social documents[74].

The attendance register records the employees' presence. This regulation only applies to a few industries, such as the diamond[75], the hospitality[76], the agricultural[77] and the truck farming[78] industries.

Special rules apply to keeping social documents for dockworkers[79]. Special rules are planned for unemployed persons assigned a place in a community work scheme[80].

2. WHO IS OBLIGED TO KEEP SOCIAL DOCUMENTS

Royal Decree no 5 has a broad scope of applicability. It applies to all employers who employ employees. Among those considered employees are:

- persons who perform work under the authority of another person even when there is no employment contract (for instance, inmates assigned work)
- persons who fall partially or completely under the social security legislation for employees (e.g. professional soccer players)
- apprentices

Civil servants employed by the federal government, by federations and agglomerations of municipalities, by provinces and by municipalities are not considered employees for the application of the regulations governing social documents. Employers employing foreign workers within the territory of Belgium are also partially exempt from the obligation to keep social documents[81].

3. FORM AND RETENTION PERIOD OF SOCIAL DOCUMENTS

Two periods in time must be distinguished in order to know what form the social documents must take. Up to a certain point, the social documents are being "maintained". Maintaining refers to recording information in the social documents and keeping them available. In a second phase, the documents must only be preserved.

3.1. MAINTAINING SOCIAL DOCUMENTS

The form in which the general and special personnel registers, the individual account, the apprentice contract for part-time pupils, the employment contract for students and domestic servants must be maintained is regulated in the Royal Decree of 8 August 1980 on keeping social documents (*Moniteur belge*, 27 August 1980).

The personnel register must be kept in the form of a bound book with consecutively numbered pages. It may consist of several bound books if lack of space prevents the required information from being recorded in a previous volume. In that case the page and employee numbers must continue in subsequent volumes (art. 4 §2 of the Royal Decree of 8 August 1980).

The special personnel register may be kept on a paper or electronic medium on the condition that the inspection can inspect it at the workplace at all times (art. 11 §2, par. 2 of the Royal Decree of 8 August 1980). There are no further formal requirements.

There is no regulated form for the individual account or for the employment contract for students and domestic servants. The same applies to the apprentice contract for part-time pupils. The employer may establish his own form. The document must contain all the mandatory information. The employer must provide the employee with a copy of the individual account before the first of March of the following year.

A Royal Decree of 17 June 1994 (*Moniteur belge* 25 June 1994) stipulates the form of the attendance register. In principle, it consists of bound and consecutively numbered monthly sheets. It must be drafted by calendar year. The list of those present must be legible and recorded in the register in indelible ink (art. 4 Royal Decree of 17 June 1994). The blank attendance registers must be certified and delivered by the body indicated for the purpose in the regulations specific to the industry sector in question.

3.2. PRESERVING SOCIAL DOCUMENTS

The employer may preserve social documents in original form or in any kind of reproduction, on the condition that it is easy to read and that the reproduction method used permits efficient inspection[82]. The storage period is 5 years starting from:

- the date that the last mandatory information was recorded, for the general and special personnel registers
- the date the agreement terminates, for individual accounts
- the day following the day after the execution of the contract ends, for employment contracts for students
- the date that the last mandatory information was recorded, for the attendance register (the storage period ends five years after the end of the month following the quarter in which the information was recorded)[83].

The retention period is not explicitly mentioned for employment contracts for domestic servants and the apprentice contract for part-time pupils. The rule applicable to the employment contract for students can be followed by analogy.

Former employers also remain subject to the obligation to preserve social documents for a given period (art. 2 Royal Decree n° 5).

4. IMMEDIATE NOTIFICATION REGARDING EMPLOYMENT (DIMONA)

An employer must report the hiring of an employee to various social security institutions, such as the child benefit institution, the industrial injuries insurer, an institute for the payment of vacation pay, etc. In addition, the social security administration often requests certain information from the employer. Although these institutions all require more or less the same information, they use a wide variety of application forms and information sheets that can only be filled in after reading voluminous instructions. To make matters even worse, the information is requested from the employer at different times of the year.

To cut down on all this paperwork, the program law of 26 July 1996[84] provided a modernization of the social security system and a simplification of the social administration. The *Dimona* project is a first step toward introducing e-government in the social security administration. The objective of the "Déclaration IMmédiate or in Dutch ONmiddellijke Aangifte" (*Dimona* [Immediate Notification]) is to provide immediate notification of the commencement and termination of employment to those government services that need it. Within the immediate notification system, the SIS (Social Information System) card offers evidence of a worker's employment under an employment contract. In the future, the immediate notification must facilitate the various social security institutions' ability to consult the Crossroads Bank for Social Security (a database for electronic data exchange) directly to locate all the information relevant for social legislation.

The immediate notification of employment was made obligatory on 1 January 1999 in the passenger transport, temporary employment and construction industries[85]. The system has been mandatory for all employers since 1 January 2003.

The *Dimona* notification must reach the National Office of Social Security (RSZ) in the form of an electronic message. Employers that do not have internet access can send their notification by using a voice server accessible by telephone. The questions presented can be answered by pressing the telephone buttons. The social security portal site offers the possibility to provide notification over the internet (http://www.socialezekerheid.be). Access to internet and a standard browser is sufficient. No special software is needed. Employers with a great number of personnel and/or frequent changes in personnel can send the notification to the RSZ using structured messages. The persons in the company responsible for developing this application can consult the manual describing the fields that the structured message must contain.

The employer can also call in one of the agencies that provide support in fulfilling social security obligations (salary administration services, software developers). They act as intermediaries in submitting the *Dimona* notification. They provide various channels that the employer can use to send them the notifications after which they notify the RSZ.

An automatic receipt is sent for each *Dimona* notification. The result of the notification can be consulted on the social security portal site. The employer must store all the messages that he receives from the RSZ for six months.

One consequence of a correct *Dimona* notification is that the employer no longer has to satisfy several obligations relating to the storage of social security documents. For instance, the general personnel register need no longer be updated. The *Dimona* notification replaces each new entry in the register. Of course, the old register must still be preserved. The employer also need no longer send a copy of the employment contract for students to the labor inspection.

The e-government platform developed under the direction of the National Office of Social Security and the Crossroads Bank for Social Security is regularly expanded with new applications. It is already possible to submit part of the notification of social risks in electronic form[86]. As of 1 January 2003, the quarterly statement of salary and work time data can only be submitted electronically[87]. The notification for the National Employment and Placement Service (RVA) that an employment contract has been suspended can also be sent electronically[88]. This involves the suspension of the employment contract for reasons of technical disorder, poor weather or lack of work due to economic causes as regulated respectively in articles 49, 50 and 51 of the Employment Contract Act[89].

5. OTHER OBLIGATIONS

In addition to social documents, the employer must preserve several other documents. The most important are described in the following paragraphs.

A copy of the part-time employment contract must be kept with the work rules. The employee and employer must both sign this document. In case of a variable work schedule, the daily work schedule for each part-time employee must be posted at least five workdays in advance. This notice must be stored for one year, starting from the day on which the work schedule is no longer in effect[90]. All divergences from the normal part-time schedule, as cited in the work rules must be noted and signed by both the employee and the employer in the master document[91]. The employer may use computer procedures for this registration on the condition that a sheet is printed at least once each week and that a sheet with the data for the day can be printed immediately in the event of an inspection. The employer must store documents for the whole period that starts on the date when the last mandatory notice was registered and ends five years after the end of the month following the quarter in which the registration was made[92].

The company's occupational health service must store the medical file drafted by the company medical officer for fifteen years starting at the time that the employee leaves the company[93]. This file must be kept in a sturdy folder that can be closed on all sides. When folded shut, only certain headings may be visible on the outside; the intention here is to respect professional secrecy.

6. TOWARD AN ELECTRONIC SOCIAL FILE

Social security law has already come a long way in its evolution from a paper to an electronic social file. This development started in the administration, with the establishment of the Crossroads Bank for Social Security, and is now gradually being expanded to cover employer-employee relations. The general distribution of the electronic identity card will provide further support for this evolution.

H. *MEDICAL FILES*

1. OBLIGATION TO PRESERVE

In the relationship between a doctor and his patient a great amount of data is generated: information that the patient gives to the doctor, measurements taken by the doctor, x-rays from a radiologist, the results of blood tests, etc. It is of vital importance for the quality of health care that all health professionals maintain a reliable medical file on each patient. Efficient communication of all this data between general practitioner and other health care practitioners is indispensable in optimizing the quality, coherence and continuity of care.

Many laws and rules refer to the notion "medical file"[94]:

- Art. 9 §1 of the Patients' Rights Act of 22 August 2002 (*Moniteur belge* 26 September 2002) gives the patient the right to a conscientiously maintained and securely stored patient file.
- The Royal Decree of 3 May 1999 on the minimal requirements applicable to the medical file in general, as referred to in art. 15 of the Hospital Act (*Moniteur belge* 30 July 1999), stipulates that a medical file must be created for each patient treated.
- The Royal Decree of 3 May 1999 on the General Medical File (*Moniteur belge* 17 July 1999) requires every patient to have a medical file managed by a general practitioner.
- Art.38 of the Medical Code of Ethics stipulates that, in principle, the doctor must keep a medical file for each patient.
- According to art. 146 quinquies §1 of the General Health and Safety Regulation (A.R.A.B./R.G.P.T.), each industrial doctor must create a medical file for each patient that he/she examines.

The term "medical file" is not defined clearly anywhere. The law just imposes certain obligations to create a medical file and describes what it must contain as conditions for the accreditation of numerous hospital services[95]. The Belgian Medical Association's professional code contains a chapter on the medical file[96].

The medical file has three functions: it is an important tool for the doctor, it serves as evidence in disputes about medical liability and, in the long term, it is a source of information for academic research. In practice there are great differences in the way doctors keep their medical files. Each doctor has his/her own habits and often his/her own specialization. In 2002, already many doctors used a computer to process their patients' medical data[97].

2. PRESERVATION PERIOD

The law provides no uniform rules regarding the preservation period for medical files. The Royal Decree of 3 May 1999, referred to above, on the medical file in hospitals[98] imposes a minimal preservation period of thirty years. The professional code also states that medical files must be preserved for thirty years after the last contact with the patient[99]. These stipulations are based on the indemnity period for personal actions provided by civil law, which, until recently, extended to thirty years. Not long ago this period was reduced.

In principle, contractual obligations and other personal actions now expire after 10 years[100]. It is quite possible for a doctor to make an error when treating a patient that cannot be considered a failure to fulfill his contractual obligations. In such cases claims for compensation for damages based on the doctor's extra-contractual liability expire after five years. However, this term only starts when the patient learns of the damage and the identity of the doctor responsible for the damage. In any event, this claim expires twenty years after the treatment. If the patient was a minor when the error occurred, all these periods commence only when he/she reaches majority. In extreme cases, the period of limitation can span 38 years. Additionally, the doctor may also be subject to criminal prosecution for involuntary assault and battery. In that case, the patient can still submit a civil claim as long as the criminal judge has not made a final decision, even if this should take more than twenty years[101] (which occurs only very exceptionally).

Some actions cause a running term of limitation to be suspended or to be restarted. In practice this means that it cannot be unambiguously ascertained how long medical documents could be useful as evidence in questions of liability. It can take years for the adverse consequences of an incorrect treatment to appear. Preserving a medical file for 30 years will suffice in many cases, but will prove insufficient in some cases. This is true from both the medical and the civil law perspectives.

Sometimes it can take years after the treatment for the effects of a medicine to appear. It is often advisable to preserve files relating to chronic and heredity disorders for decades[102]. Of course, this has consequences for the size of the archives. An electronic medical file can alleviate this problem.

A medical file contains primarily factual material; hence it is subject to the unrestricted evidence system. There is no regulation which states that the medical file must be preserved in its original form. Nothing prevents preservation on microfilm or in electronic form. The doctor must be able to convince the judge that the data are real and not falsifications, regardless of the form of the medical file.

3. TOWARD AN ELECTRONIC HEALTH NETWORK

As part of the modernization of health care, the government has taken various steps toward an electronic health network and a shared patient file accessible to all health practitioners treating the patient.

The comprehensive medical file was introduced as the first step in this evolution[103]. All the information relating to the patient's state of health is centralized in this file. The general practitioner chosen by the patient manages the comprehensive medical file. The intention of this system is to improve the quality of health care greatly by centralizing medical data so that it can be processed more efficiently, with the general practitioner as pivotal figure. This allows all those involved to follow up on the patient's state of health more efficiently. For instance, ordering the same test twice can be avoided. Up to now the patient may decide freely whether or not to allow a comprehensive medical file to be created.

The comprehensive medical file can only be used efficiently in the health care network when the information is maintained and archived in electronic form. This way everyone involved can have rapid access to the data when necessary. Nevertheless, the law still allows doctors to maintain the file in paper form in stead of electronically.

The "Telematics Standardization Commission For Health Care"[104] (hereinafter referred to as "the Telematics Commission") was set up to avoid chaos in the electronic exchange of medical data, to ensure system interoperability and to guarantee the confidential and secure handling of medical data. A telematics cell was also established within the Federal Public Service for Social Affairs, Public Health and the Environment to help achieve these goals.

The Telematics Commission was assigned the task of developing modalities for the electronic exchange of medical data. However, it had no regulatory authority. The official regulatory authority rests with the BIN (Belgian Institute for Normalization), with the CEN (European Committee for Normalization) and the ISO (International Organization for Standardization).

The Telematics Commission developed quality criteria for computer systems used by hospitals and general practitioners. The EMDMI (*Elektronisch Medisch Dossier Médical Informatisé* [Electronic Medical File]) working group of the Federal Public Service for Social Affairs, Public Health and the Environment developed quality criteria for software applications designed to manage patient files for general practitioners. Software producers can submit their programs to a certification procedure to obtain a quality label. The commission issued several recommendations relating to the preservation of medical files, specifically regarding the content of the file, the preservation period, and the form[105].

Additionnally recommendations were issued to standardize and harmonise the content, the exchange formats and syntax of electronic messages to allow a consistent integration of data in the comprehensive electronic medical file[106]. Finally, guidelines were formulated for the use of the electronic signature so that all persons concerned could be identified unambiguously. In this way, the origin of the information in the file can be verified and access to it restricted.

4. PROTECTING PRIVACY

Medical data are not like other data, but are highly sensitive data which are protected by the patient's right to privacy. No one would welcome having his/her medical file open to the perusal of just anyone. For this reason special care must be taken when processing medical information.

The Privacy Act and the Patients' Rights Act regulate the processing of medical data. Personal information relating to the former, present or future state of a patient's physical or mental health is medical information as defined in the Privacy Act. In principle, it is forbidden to process medical information. The only exceptions to this prohibition are those cases listed in the Privacy Act, for instance to create a medical file[107]. But there are several conditions that must be observed.

Medical information must be processed under the supervision of a health care professional. This refers to all persons who provide health care to others as part of their professional activity. This category is much broader than the category of persons that medical law obliges to maintain a medical file.

Persons processing medical information are subject to a confidentiality obligation.Most health practitioners are already subject to other confidentiality rules, for instance, the professional secrecy proscribed by art 458 of the Belgian Penal Code or the duty of confidentiality in the professional code. Art. 39 3° of the Privacy Act also punishes breach of confidentiality as a criminal offence.

Medical information must be obtained from the person whom it concerns. This principle must prevent medical information used to provide a treatment from being collected from a variety of sources, such as other health care professionals, without the knowledge of the person concerned.

The Patients' Rights Act reaffirms the patient's right to the protection of his privacy in each intervention by a health care professional, and in particular with regard to information relating to his state of health[108]. This act elaborates the right of access to one's own medical information granted in the Privacy Act. The patient has the right to consult his file, with the exception of the personal notes made by the health care professional and the information relating to third parties. If desired, the patient can seek the support of a confidential counselor or request that a confidential counselor of his choice be allowed to consult the information. If this person is a health care professional, he/she will also be allowed to consult the personal notes.

Insofar as the health practitioner believes that consultation of the file would manifestly affect the patient's health in an adverse way, he can refuse to provide access to the patient. In that case, the patient can appoint another health care professional to consult the file on his/her behalf, including the personal notes.

The patient has the right to a copy of all or part of his file, under the same conditions as the right to consultation. Each copy mentions that it is strictly personal and confidential. The health care provider can refuse to give a copy if he/she has clear indications that third parties have put the patient under pressure to obtain a copy of his file.

After the patient's death, the patient's spouse, civil registered partner, partner and blood relatives to the second degree may appoint a health practitioner to consult the deceased's file on their behalf, if their request is sufficiently motivated and specific and the patient had not expressly objected to this.

Every document management system used to maintain and preserve medical files must respect the privacy of those concerned.

5. FRAGMENTED MEDICAL FILE

Every health care professional keeps a file on his/her patients and many already use electronic files. Each of these files is generally completely independent and is not co-ordinated in any way. Through the development of standards and the recommendations, the government is trying to lay the foundation for an electronic health network that will allow files relating to a given patient to be linked to one another. The protection of the privacy of all those concerned is the greatest challenge here.

I. PRIVACY

The right to privacy encompasses the right to engage in relationships with others without the interference of third parties. This fundamental right has far-reaching implications and has many incarnations in our law.

Historically, this law arose as a defensive right against interference from the government. However, experience has shown that we have as much to fear from our peers. The rise of information technology has acerbated the issue of privacy protection.

Privacy regulation has a far-reaching impact on all aspects of archiving. The inclusion of documents in the archive may only happen in compliance with the right to privacy of all involved. The confidentiality of the data in the archive must be guaranteed and unlawful modifications must be avoided. Consultation of personal data in the archive and making them available to third parties are strictly regulated.

The law on the Protection of Personal Privacy (Data Processing) Act, which establishes a general framework in our country, will be discussed below. Only those aspects that are important for digital archiving are elucidated[109].

1. SCOPE OF THE PRIVACY ACT

1.1. DATA CONTROLLER

Any processing of personal information carried out within the territory of Belgium, by someone domiciled here, must satisfy the conditions imposed by the law[110]. The Privacy Act applies to the government, private organizations and citizens alike.

The obligations imposed by the law are aimed at “those responsible for processing". This is the person who, alone or with others, determines the objectives of and means used for processing personal data[111]. If the objective and the means for processing have been established by or in execution of a law, a decree or an ordinance, the data controller is the person or entity indicated by this norm. Generally, the records creator, in other words, the person who decided to archive documents and information, is the data controller and as such he/she bears responsibility for compliance with the privacy rules.

The data controller can call upon the aid of a "processor". "Processor" here means the one who actually processes the personal at the behest and under the supervision of the data controller[112]. This is the case when the archive is contracted out to a third party. The employees or subordinates of the data controller are not "processors" in the sense of the Privacy Act.

1.2. PERSONAL DATA

"Personal data" is any type of information relating to an identified or identifiable natural person, the data subject. A person is "identifiable" if he/she can be identified directly or indirectly, in particular by means of an identification number or of one or more specific elements characteristic of his/her physical, physiological, mental, economic, cultural or social identity[113].

The term "personal data" must be interpreted very broadly. It is not required that the person holding the information can identify the data subject. As soon as *anyone* is able to identify the person concerned using reasonable means, the information is considered personal data. For instance, an e-mail address with a pseudonym (for example incognito@provider.be) does not immediately reveal the owner of the address. The service provider probably knows which of its customers uses this alias. In that case, an e-mail address is personal data concerning the customer, regardless of who processes the address.

By "processing" is meant any manipulation or any series of manipulations performed on or with the personal data, whether or not implemented with the help of automated procedures such as the collecting, recording, ordering, storing, updating, modifying, retrieving, consulting, using, providing by passing on, distributing or making them available in any other way, collating, co-ordinating as well as restricting, deleting or destroying personal data[114]. This term, too, must be interpreted broadly. The law applies to every process that occurs in whole or in part automatically, and to some manual processing[115].

The law applies only to a limited degree to processing carried out by the security, police or intelligence services[116]. The European Centre for Missing and Sexually Exploited Children was granted a few exceptions[117]. Additional exemptions can be granted by royal decree. These exemptions primarily impact the creation of archives, and have only a limited effect on the archive management by the archivist.

2. BASIC PRINCIPLES OF THE PRIVACY ACT

Three important principles lay at the basis of the Privacy Act: legality or transparency, finality and proportionality. In each case, the provisions of the Act elaborate the practical effects of these principles.

2.1. LEGALITY OR TRANSPARENCY

The legality or transparency principle signifies that anyone must reasonably be able to know what information is being processed about him or her, why this is being done and who is doing it. The data controller must provide clear information so that all those concerned are reasonably aware of which privacy expectations they may harbor.

In the first place, the law establishes under which conditions it is permissible to process personal data. The following situations are important for the private sector:

- the person concerned has given his/her unequivocal consent[118]
- the processing is necessary to comply with an agreement to which the data subject is a party or to take measures prior to the closing of this agreement when done at the request of the person concerned[119]
- the processing is necessary to fulfill an obligation to which the data controller is subjected by a law, a decree or an ordinance, or by an executory measure[120]
- the processing is necessary in pursuit of a justified interest of the data controller or of the third party to whom the data is given, except when the interests or the fundamental rights and freedoms of the person involved outweigh the data controllers interest[121]. The King is authorized to exclude application of this rule in certain cases.

2.2. FINALITY

The principle of finality signifies that personal data may only be processed for a very specific, explicitly defined and justifiable purpose. Using the data for a different purpose is only permitted if this new purpose is compatible with the original one. The compatibility must be evaluated taking into account all relevant factors, specifically the reasonable expectations of the data subject, and the applicable laws and regulations[122]. Further processing of the data for historical, statistical or academic purposes are not considered incompatible under the conditions established by Royal Decree[123]. Collecting information because it may come in handy some day is out of the question.

2.3. PROPORTIONALITY

Only information that is really necessary to attain the objectives set may be processed: the data must be sufficient, relevant and may not be excessive[124]. On top of this, the information must be accurate and, if necessary, updated[125]. This does not imply that the original document must be modified, alternatively remarks may be added in an annex.

Personal data may not be stored in an identifiable way longer than necessary.[126] The Privacy Decree contains a special regime for historical, statistical or academic purposes. When selecting documents for the archives, the proportionality principle will have an important role to play.

3. DATA SUBJECT PROTECTION RIGHTS

3.1. NOTIFICATION RIGHT

The data controller must, in principle, notify all data subjects that information about them is being processed. The law makes a distinction depending on whether the information came from the data subject himself or from another source.

3.1.1. Data Received from Data Subject

An organization will mainly archive personal data requested directly from the data subject. Examples of this are the personnel files or customer information.

In principle, the data subject must be notified about the objective and the context of the processing at the latest upon the time of collection, except if he is already aware of this information[127]. Additional obligations can be proscribed for specific situations by royal decree. The notification should specifically contain the following information:

- the name and address of the person responsible for the processing and, where appropriate, his representative
- the purposes of the processing
- the recipients or the categories of recipients of the data
- information on whether an answer is mandatory and the possible consequences of not providing an answer
- a notice that the person concerned has the right to consult and correct his/her own personal data.

Personal data may only be preserved for as long as they are required in order to achieve the purposes for which they were collected. When archiving is a goal in itself, the organization should state this when collecting the information.

3.1.2. Data Received from Another Source

When the data has not been received from data subject, there is no immediate occasion to provide the required notification. The law gives data controller several options: either he/she contacts the data subject immediately after receiving the information, or he/she does so before passing on the information to third parties. Again, in specific cases, a royal decree may proscribe additional obligations.

The notification must contain the following information:

- the name and address of the data controller and, where appropriate, his representative
- the purposes of the processing
- notice that the data subject has the right, upon request and at no cost, to oppose the processing of his personal data for the purpose of direct marketing. In this case, the person must be informed before the personal data are given to a third party for the first time or before they are used for the first time in direct marketing for the benefit of third parties.
- the categories of data involved
- the recipients or categories of recipients

- a notice that the person concerned has the right to consult and correct his/her own personal data.

There are various exceptions to this rule. When the data subject already has the necessary information about the data processing, the data controller need not provide a new notification[128].

If the personal data is recorded or transmitted in order to compliance with the law[129], no notification is required[130].

The data controller is not obliged to notify when this is impossible or when this would require a disproportionate amount of effort[131]. The Privacy Decree[132] imposes additional conditions upon this exception, which is primarily intended for data processing in the public interest, such as statistical, historical or academic research or for population studies with a view to protecting and improving public health.

3.2. COMMUNICATION RIGHT

The Privacy Act gives everyone the right to determine how his/her personal data are used. First and foremost, any data subject has the right to ask whether information about him/her is being processed. If this is the case, the data controller must also provide information about the objectives of this processing, about the categories of data in question and about the categories of recipients to whom the information is given[133].

Moreover, the data subject may demand that the data involved is communicated to him in an accessible form. Any information available about the origin of the data must be included[134]. In legal doctrine, a pragmatic interpretation of this obligation is advocated. If it requires a disproportionately great effort to make a copy of all the data, an overview should suffice[135].

This obligation imposes a heavy burden on the management of archives. As the notion "personal data" is interpreted very broadly, many people can invoke this right. For example, a personnel file mainly contains personal data about the employee concerned. However, the same file may also contain information about the members of his/her family, evaluations from his superiors, information about the human resource manager and correspondence with various social security agencies. One personnel file can thus contain personal data about many different people. Ideally, the metadata to each document or file in the archive should contain a list of all the data subjects involved. Ideally such a list is recorded from the very moment the document or file is created.

To exercise the communication right, the data subject must send a dated and signed request to the data controller, his representative in Belgium or the processor. The data subject must prove his/her identity. The request may be delivered by hand, post or electronically. If the request is delivered by hand, the clerk must immediately hand over a dated and signed receipt. The data controller must respond to the request within 45 days of receiving it[136].

There are only a few exceptions to the communication right, namely for data processing by the government bodies listed in the law . In some cases there is no direct right to be informed, but those concerned must apply to the *Commission for the Protection of Privacy*[138].

3.3. CORRECTION RIGHT

Everyone has the right to have all incorrect personal data relating to him/her corrected at no cost. In addition to correcting inaccurate data, the person concerned may also provide supplementary information. When information is processed in contravention of the law, he/she may demand that it be deleted, or at least no longer used[139].

The data subject may not simply replace subjective evaluations with his/her own version, but the data controller must record that the information is challenged[140]. In other cases, too, it can be advisable not to make changes and additions to the original document but to place them in an annex.

The right to make corrections can be invoked in the same way as the communication right. The data controller has a month to respond. In his/her answer a list of the corrections or deletions must be included. This information is also passed on to the third parties to whom he/she has transmitted incorrect, incomplete or irrelevant data insofar as the data controller still knows to whom the data was transmitted. This obligation does not apply when this notification is impossible or requires a disproportionately great effort[141].

There are only a few exceptions to the right to make corrections, again for those government bodies listed in the law[142]. In this case, too, the right to make corrections must sometimes be exercised through the Commission for the Protection of Privacy[143].

3.4. RIGHT TO OBJECT

Every data subject may object to the processing of his/her personal data if he/she has weighty and justified reasons for doing so[144]. One may object to processing for direct marketing purposes without any specific motivation[145]. When collecting data, the data controller must give the data subject an opportunity to object to the use of his/her details for direct marketing[146].

The right to object does not apply when the processing is necessary:

- to fulfill a obligation prescribed by law to which data controller is subject, or
- to execute an agreement to which the person concerned is a party or in order to to take measures which were requested by the data subject in preperation of contract conlusion[147]

The records creator can record the legal basis for processing the personal data in the metadata. This way it can be easily determined later on whether or not a right to object exists.

The procedure for invoking the right to object is the same as for the correction right. The data controller must notify the requestor within a month about what action he will take[148].

In addition to those already mentioned, there are a few other exceptions for some public bodies[149]. In some cases the right to object may be exercised indirectly via the Commission for the Protection of Privacy[150].

3.5. RIGHT TO REDRESS

The Privacy Act gives the data subject two special remedies against violations of his/her privacy. The data subject can file a complaint with the president of the court of first instance or can lodge a complaint to the Commission for the Protection of Privacy[151]. In addition the data subject can, of course, also use regular legal remedies, such as lodging a complaint with the district attorney, suing for civil action concurrent with a criminal complaint or submitting a claim for damages to a civil court.

4. PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA

In addition to the rules already discussed, there is a more stringent regime for several special cases of personal data[152]. In principle, it is totally forbidden to process such information, except in the cases described in the law. In what follows the guiding principles of the law are explained.

The Privacy Decree establishes conditions for the various special categories of data[153]. The data controller must indicate the categories of persons who can consult the data and describe their task in processing the data. This also applies to cases in which a processor is brought in. The data controller must ensure that the persons indicated are bound by a legal, statutory or contractual confidentiality obligation. The notification to the data subject and the registration with the commission must cite the legal ground invoked by the data controller for the processing.

4.1. SENSITIVE DATA

Personal data revealing the racial or ethnic origin, political convictions, religious or philosophical convictions or union membership, as well as personal data regarding sexual orientation all fall under the category "sensitive information"[154].

Sensitive information may be processed in among others the following cases[155]:

- The data subject has given written permission for such processing, on the condition that he/she may withdraw this permission at any time. This exception cannot be invoked by present or potential employers of the data subject, or by any person with whom the he/she is in a position of dependence, unless the object of the processing is to provide a benefit.
- The processing is necessary to allow the data controller to comply with specific obligations and rights relating to labor law;
- The processing is necessary for the realization of an objective established by or by virtue of the laws governing social security;
- The processing relates to information that the data subject has indisputably made public;
- The processing is necessary for the establishment, exercise or defense of a right in court;
- The processing is necessary for academic research, insofar as the conditions established in the Royal Decree are met.

Sensitive information may also be processed in other cases when a law, decree or ordinance permits this for another important reason relating to a public interest[156]. A royal decree or a ministerial order does not suffice in this case.

4.2. MEDICAL INFORMATION

This category covers all information related to health[157]. The law does not explain this term further, but it refers to "all personal information relating to the former, present or future state of a person's physical or mental health"[158].

Medical information may be processed in the following cases[159]:

- The data subject has given written permission for such processing, on the condition that he/she may withdraw this permission at any time. This exception cannot be invoked by present or potential employers of the data subject, or by any person with whom the he/she is in a position of dependence, unless the object of the processing is to provide a benefit.
- The processing is necessary to allow the data controller to comply with specific obligations and rights relating to labor law;
- The processing is necessary to reach an objective established by or by virtue of the laws governing social security.
- The processing is necessary for preventative medicine or medical diagnosis, to provide care or treatment to the data subject or a relative, or for the management of medical services in the interests of the data subject. The data must be processed under the supervision of a health care professional who is subject to an obligation of secrecy.
- The processing involves information that the person concerned has indisputably made public.
- The processing is necessary to establish, exercise or defend a right in court.
- When the processing is necessary for academic research, insofar as the conditions established in the Royal Decree are met.

Beyond these specific cases, medical information may be processed in all cases in which this is required by a law, decree, ordinance, a royal decree or a ministerial order for reasons of grave public interest[160]. All processing must be done under the supervision of a health care professional bound by secrecy[161]. Moreover, medical information must, in principle, be obtained from the data subject himself. Requesting medical information from third parties is only allowed when this is the only justifiable option[162].

The data subject also has a right to have his medical information communicated to him/her. Both he and the data controller can request that the information be consulted through the mediation of a doctor or other professional health care professional[163]. The exercise of this right is regulated further by the Patients' Rights Act[164].

4.3. JUDICIAL INFORMATION

Personal data relating to disputes submitted to tribunals and courts as well as to administrative tribunals, relating to accusations, prosecutions or judgments dealing with criminal offences or relating to administrative penalties or security measures are all considered judicial information[165].

The following are among the exceptional cases when judicial information may be processed[166]:

- The processing is necessary for the management of the data subject's own disputes or those of the data controller.
- The processing is necessary for academic research, insofar as the conditions established in the Royal Decree are met.

Judicial information may be processed if this is necessary to achieve the objectives that a law, decree or ordinance, a royal decree or a ministerial order has established[167].

In cases where the data controller is allowed to process judicial information, he is bound by an obligation of secrecy.

4.4. ARCHIVING SENSITIVE, MEDICAL AND JUDICIAL INFORMATION

The initial gathering and processing of these special categories of information must fall within the scope of one of the exceptions listed in the Privacy Act and must satisfy the numerous conditions that are set. The preservation of this information must also be justifiable on the same or another legal basis.

Communicating special personal data is, in itself, a type of processing and is only possible when the legal basis invoked justifies this. To the extent that archiving takes place internally (by subordinates or by a processor) this is not an issue, as there is no communication to third parties going on. All employees must be bound an obligation of confidentiality.

Granting access to the archives is an entirely different situation. There must be a legal basis for the communication of the data. The Privacy Act permits communication in relation to a legal dispute one is involved in or for academic research, albeit under the conditions established by Royal Decree[168].

In order to be able to comply with the stipulations of the Privacy Act efficiently, the metadata of documents and files in the archive should mention whether they contain sensitive, medical or judicial information.

5. ADMINISTRATIVE PROVISIONS

5.1. REGISTRATION

The data controller must register his activities with the Commission for the Protection of Privacy before he starts processing personal information[169]. There are many exceptions to this rule, in order to limit the amount of registrations[170]. Among the exemptions are processing as part of salary administration, personnel administration, accounting, customer and supplier relationship management, municipal registers and processing by government administrations[171]. The Privacy Decree imposes special conditions in each case.

5.2. AUTHORISATION BY THE COMPETENT SECTORAL COMMITTEE

As of 2003, the law allows sectoral committees to be established within the commission. These sectoral committees are competent to examine and decide upon all requests relating to the processing or communication of information governed by any special legislation[172]. An existing example is the sectoral committee for social security[173] and the sectoral committee for the federal government established by the Privacy Act[174]. In principle, any time the federal government wishes to communicate personal data, authorization is required from the federal sectoral committee, which investigates whether the communication complies with the laws and rules[175].

6. MISCELLANEOUS PROVISIONS

The Privacy Act regulates various other aspects of the processing of personal data. A short overview is given here for the sake of completeness. Only aspects that are of specific importance for digital archiving are elaborated further.

6.1. SECURITY AND CONFIDENTIALITY OF DATA PROCESSING

The data controller must take suitable technical and organizational measures to protect personal data against fortuitous or wrongful destruction, accidental loss, modification, unlawful access and any unlawful processing in general. An appropriate level of security must be guaranteed given the state of the art in technology, the costs involved, the nature of the data to be protected and the potential risks[176]. In other words, the data controller must guarantee the confidentiality and integrity of the information.

The Privacy Act lists several specific objectives that data controller must satisfy. A procedure should be in place for updating information so that incorrect, incomplete, irrelevant and unlawfully obtained or processed information can be corrected or removed. Access to the data and processing tools may only be entrusted to employees and other subordinates to the extent necessary for the execution of their responsibilities and the operational needs of the organization. The employees concerned must be educated about the applicable privacy regulations. The actual processing of information must correspond to the activities mentionned in the registration to the Privacy Commission[177].

If the data controller out-sources certain tasks, he must choose a processor that guarantees a sufficient level of security. The out-sourcing contract must describe the technical and organizational security measures, as well as the liability of the processor in the event of non-compliance. Also, the contract impose upon the processor the same privacy obligations as those to which the data controller is bound. The contract must be drafted in writing, on paper or in electronic form[178].

6.2. CROSS-BORDER DATA EXCHANGE

The law regulates the transmission of data to third countries more stringently than exchange of data among EU countries. In many countries, a much lower standard of protection for personal data is in place[179].

The question whether the level of protection is sufficient in a certain country can not be answered in general. Each case must be examined individually, taking into account the nature of the data, the objectives and the duration of the intended processing, the countries of origin and destination, the general and sectoral legislation in these countries, as well as the professional codes and protective measures observed in these countries.

Under certain circumstances, data may still be exchanged with countries lacking a suitable level of protection. This is the case when all those involved have given their unequivocal permission or when the information is used in preparation of or in the execution of a contract with the data subject. This is also allowed in order to defend a right in a legal dispute or when this is prescribed by Belgian law[180].

The data controller himself can guarantee sufficient protection, for instance by including privacy protection obligations in the contract with the foreign recipient. After authorization from the King, the personal data may then be transmitted[181].

6.3. PENALTY PROVISIONS

Articles 37-43 of the Privacy Act impose a fine on infringements of the law. In addition to imposing a fine, the judge can order the confiscation of the media containing the personal data involved in the crime, such as paper files, magnetic disks or tapes, with the exception of the computers or any other equipment, or can order that the data be deleted from them. The confiscation or the deletion can be ordered even when the media in question do not belong to the person convicted[182].

7. CASE STUDY: ARCHIVING PROFESSIONAL E-MAIL

Correspondence in paper form is routinely classified and archived in most organizations. Likewise, business-related e-mail should be included in the archives as well. From a technical point of view it is feasible to preserve all incoming and outgoing messages. However, this practice would raise many hairy questions from a legal perspective.

7.1. FREEDOM OF COMMUNICATION

The right to privacy is not limited to a right to be left alone, but includes the right to engage in relationships with others without interference from third parties. "Interference" encompasses preventing or hampering communication as well as monitoring communication. This aspect of the right to privacy is called the freedom of communication.

The freedom of communication is of such importance in our society that numerous protective rules have been enacted[183]. Letters fall under the confidentiality of correspondence.[184] Telecommunication, including telephone conversations, SMS and e-mail fall under the confidentiality of telecommunication. The more general rules of the Privacy Act also apply, except where more specific regulation diverges.

The confidentiality of telecommunication not only forbids outsiders to read the content of someone else's e-mail, but even to record the fact that messages are exchanged. Using a device to intercept private messages during transmission constitutes illegal wiretapping[185]. Interception is only punishable if it is done intentionally, meaning knowingly and willingly[186]. In this context, "private" means that the message is not intended to be read by everyone. In principle, professional e-mail also has a private character as it is not directed at the public at large[187].

Monitoring someone else's communications, even without accessing the content, is a seperate offence[188]. This monitoring need involve no more than recording the name of the correspondents, the subject of the e-mail, the time of sending, whether or not there was an attachment and any other information regarding the telecommunication.

The confidentiality of telecommunication entails that an employee's e-mail may not be added to the company archive just like that. An absolute prohibition on accessing an employee's mailbox is untenable in a professional context. On the one hand the employer feels the need to supervise the use that his employees make of e-mail. On the other hand, important business information must be accessible to the company. For instance, communication via e-mail is increasingly being used as evidence in court.

Confidentiality of telecommunication is not an absolute right. In cases where all the participants to a communication give permission for the interference, no offence is committed. In addition, there is an exception for cases where a law permits or requires the interference[189]. This exception is primarily intended to allow wiretapping as part of a criminal inquiry, as circumscribed in the Wiretap Regulation[190]. Some legal scholars[191] see another example in the relationship of subordination between the employee and his/her employer[192]. On this basis, the employer may monitor the employee's use of internet and e-mail, and may also set up an archive containing professional messages. Nonetheless, the Privacy Act still applies and determines the limits the employer must respect when exercising his supervision.

7.2. COLLECTIVE LABOR AGREEMENT (CLA) NO 81 ON THE PROTECTION OF PRIVACY IN THE MONITORING OF ELECTRONIC ONLINE COMMUNICATION DATA

Thus far, the monitoring of abuse of e-mail and internet facilities at work has received more attention than the issue of archiving. Concerns about monitoring both on the part of employers as of employees led to the negotiation of CLA no 81[193]. The employers' organizations and the trade unions looked at all the applicable legislation and applied these to work environment in a way that balances the interests at stake. Although this was not the CLA's primary intention, the agreement does have an impact on archiving professional e-mail in the private sector[194].

The CLA elaborates the three basic principles from the Privacy Act, namely, transparency, finality and proportionality. The employer must take these principles into account when he sets up an archiving system as well as during its use.

In a first phase, the employer must delineate a detailed archival policy, which establishes the categories of e-mail messages to be saved as well as the metadata[195] to be added to each message. The archival policy should explain to the employees what to archive and how to do this. At the same time this gives employees an idea of which type of personal data will be kept in the archive. Also, the system put in place to monitor compliance with the archival policy must be explained. The information supplied describe how the monitoring will be carried out, the prerogatives of supervisors, the objectives pursued, the place and duration of the preservation of personal data, whether or not monitoring is permanent or happens sporadically, and whether any penalties will be imposed[196].

By virtue of the proportionality principle, only professional e-mail may be preserved in the archives. In general, private e-mail is of no interest to the company and therefor preserving such messages in an archive where colleagues may consult them is a violation of privacy. In the CLA the distinction between "private" end "professional" e-mail is made, although these terms are given a specific meaning. Basically all e-mail is considered private except when the employee "does not cast doubt" upon its professional nature. This description is extremely vague and difficult to apply in practice. The employer would do well to ask his employees to indicate explicitly for each outgoing and incoming message whether or not it is professional[197]. According to the CLA, professional e-mail may be archived without further ado for future use within the company. Private e-mail may only be consulted in a limited number of cases, for instance in order to monitor abuse.

The monitoring of the use made by employees of e-mail and internet must be executed in two distinct phases[198]; the same applies to monitoring of compliance with the archival policy. In the first phase, the monitoring should be done at a general level and only anonymous data should be processed. In case this brings to light evidence of non-compliance with the archival policy, the employer should explain the policy again to his personnel and warn them that if a similar violation occurs in the future, those responsible will be identified. Tracing breaches back to the individual responsible is the second phase, in which case even "private" e-mail – as defined in the CLA – may be perused. This procedure shows that the CLA is primarily aimed at restraining abuse and not at supporting normal business processes, such as archiving professional information. Assessing the archival value of e-mail anonymously is extremely difficult. Organizations should put at least as much effort into encouraging employees to archive information, as in monitoring their behavior.

The CLA only covers the relationship between the employer and his employees, without giving any regard to the position of third parties, for instance business contacts. In any case, the rules of the Privacy Act must be respected with regard to these third parties. Thus, the correspondents must be informed about the processing of their data. This can be done by including a notice to this effect at the bottom of each outgoing e-mail message. An automatic response with this information could also be sent to new correspondents contacting the organization spontaneously.

8. ARCHIVING IS PERSONAL DATA MANAGEMENT

Every organization must set up its information systems taking into account the requirements of the Privacy Act. Likewise, it should ensure that the recipients of its information are also able to comply with the legal provisions. The organization can satisfy this requirement by adding certain metadata to its documents, for instance, a list of data subjects, the nature of the information, which notification was made, …

Implementing privacy regulation in practice is a complex matter. It is essential to draft a well-considered privacy policy. Processing information in contravention of the law can have grave consequences, as the data involved must, in principle, be destroyed.

J. COPYRIGHT AND NEIGHBORING RIGHTS

1. INTRODUCTION

In the paper environment, copyright law had little impact on the activities of the records manager. Preserving a physical copy of a work and making it available for consultation are not activities relevant to copyright law. With digital archiving, the situation is very different as each use of a digital work requires the production of copies. In what follows the guiding principles of copyright law, including the specific rules for computer programs and databases, are explained insofar as is relevant for archiving in the private sector.

In addition to the author, other intermediaries play a role in the exploitation of a work. Some of these intermediaries enjoy a right neighboring to copyright, for instance performing artists, the producer of phonograms and films, broadcasting companies and the producer of databases. Only the *sui generis* right of the database producer will be elucidated in any detail, as this is relevant for every archive.[199]

2. SCOPE OF APPLICATION

Copyright law protects texts, images, musical compositions, computer programs and any other work, as long as the work possess a minimal degree of originality and has been shaped into a particular form. These two conditions will be explained briefly.

2.1. ORIGINALITY

An original work is the result of the intellectual activity or effort of its creator. The effort need not be very great, but must only be demonstrable. Originality presupposes that the personality of the creator is expressed in the work in some way. In other words, from the range of possibilities, the creator has chosen one form of expression according to his/her personal preference.

Original does not necessarily imply "new": different people can reach similar results independently. When many people express the same idea in the same manner, the work may be considered "banal" and is not protected by copyright. The amount of similar results suggests that the work is not an expression of the creator's personality.

2.2. FORM

Ideas are not protected by copyright because ideas cannot be communicated directly to others. Ideas must be expressed or put into a particular form and it is only this expression or form which can be protected.

The artist Christo is world renown for wrapping large structures in cloth, such as the Pont-Neuf in Paris or the parliament building in Berlin. The idea to wrap structures is not protected by copyright and anyone may imitate it.

"Form" does not mean that only tangible objects are protected. Speeches, radio programs and websites are also protected.

2.3. BUSINESS DOCUMENTS

Copyright law protects a broad spectrum of works, including material created within a professional context. An obvious example is a company's advertising material, including its website. Beside this reports, internal memos and even correspondence can be protected by copyright if they are sufficiently original. For all these documents, it is very important to determine who the copyright holder is and the extent of the protection.

In principle, business figures, telephone lists and the like are not protected by copyright. But the presentation and ordering of the material can be protected if it is sufficiently original. The content may even fall under the *sui generis* database protection right.

3. THE COPYRIGHT HOLDER

The person who created the work is the initial copyright holder or author. The copyright will often be held by someone else; the author can yield his/her rights in a contract and at death, his/her heirs inherit them. The law uses the term "author" to designate both the original creator of a work and all persons who have received this right from him/her. In what follows the term "author" will also be used to designate all copyright holders.

For an outsider, it is very difficult to identify the copyright holder at a given time. The law provides that the person whose name or "acronym" is mentioned on the work may be presumed to be the actual copyright holder. In case of an anonymous work, the "publisher" is presumed to exercise control over the copyrights. The term "publisher" includes anyone who manufactures works protected by copyright and puts them on the market.

A company or organization generally knows who created its advertising material, reports and the like. Therefor the board of directors cannot simply invoke the presence of the company logo on the document as a presumption of entitlement against the actual creator of the work, but must show that the latter has transferred his/her copyright to the company.

4. EXTENT OF THE PROTECTION

The author receives two types of rights to his/her work: property rights and moral rights. The property rights give the author a monopoly on the exploitation of his/her work. The moral rights protect the "intimate bond" between the initial author and his/her creation.

4.1. PROPERTY RIGHTS

The author has the exclusive right to reproduce, distribute, rent and loan his/her work. Beside this, the author has the exclusive right to produce derivative works (for instance translations, adaptations to another medium, merchandising, etc.). Finally, the author must give his/her consent for each communication to the public (for instance broadcasting on radio or television, performance of a play).

In the traditional analogue context, the monopoly on reproduction and communication to the public cover mainly ways to exploit a work commercially. For instance, only the author may have his/her book printed and distributed for sale. The end-user has the right to read his/her copy, to resell it and to lend it to third parties. Archiving a copy also poses no problem.

But matters are different for digital works. The end-user cannot possibly use a digital work without making several copies of it, even if this is limited to the transitory copies in the computer's working memory. In theory, the author must give his/her permission for this. Indirectly, this gives the author much more power over how the end-user may or may not use the work.

Making digital works available on a network is usually equivalent to communicating them to the public and the author's permission is therefor required. Unless an organization obtains the copyrights to works created by its employees, it must ask the author's permission each time before distribution.

Copyright law has an impact on digital archiving in various ways. The archivist or records manager must copy the work to include it in his/her archive. Over time, the work must be adapted so that it remains accessible for the future. Finally, it is also the intention to make the work available to others, either the general public or a select few.

4.2. MORAL RIGHTS

The initial author has the right of divulgation or disclosure: only he/she may decide when the work is ready to be made public. The paternity right implies that the author decides under what name the work will be published. The author can oppose any modification to his/her creation on the basis of his right to integrity.

Moral rights are strictly personal, which means that they are linked to a particular person and are not transferable. The moral rights protect the "intimate bond" between the author and his creation, which is considered an expression of his/her personality.

An organization can never be the holder of the moral right to a work, since this is not transferable. To a certain degree, the original author of a work can promise not to exercise his/her moral rights.

5. EXCEPTIONS TO COPYRIGHT

From the very beginning when copyright was first introduced in 1886, the legislator was aware that certain interests should be given precedence over the author's exclusive rights. Under certain circumstances the law grants permission to reproduce a work or make it public without the author's consent. These exceptions are also called "compulsory licenses" or "legal licenses".

Broadly speaking, the exceptions apply to private use, use as illustration in education, use for academic research and use in the public interest. Each case is subject to specific conditions in order to keep the interference with the commercial exploitation by the copyright holder to an acceptable minimum.

To some extent public and private archives can invoke these exceptions inasfar as they are not commercially active[200]. Business archives can generally not invoke these exceptions, since they are by definition operating in a commercial context. In what follows, the copyright exceptions will only be discussed where relevant to business archives.

6. TERM OF PROTECTION

Copyright protection runs until 70 years after the author's death. After his/her death, the author's rights pass to his/her heirs, unless he/she has assigned them to someone else. When a work is authored by more than one person, the copyright continues until 70 years after the death of the longest surviving author.

For anonymous or pseudonymous works, the 70-year term commences from the point in time when the work was lawfully made accessible to the public. In case the pseudonym leaves no doubt about the real identity of the author, the general rule applies.

All terms are calculated as of January 1st of the year following upon the event that gives rise to the rights. The correct calculation of the term of protection is mainly of interest for works exploited commercially, for instance a book, a play or a comic-book character. Business documents, such as advertising material and reports will generally lose their relevance long before this term has expired.

7. LICENSES

The original author is not required to exploit his work himself, he may authorize others to do so. The agreement whereby an author grants permission to a third party to exploit his work or in which ownership of copyrights are transferred, is called a "license agreement".

The Copyright Act imposes several special conditions upon licence agreements to protect the author. Only a written license agreement has evidential value against the author. The license must expressly state if and how the author will be remunerated, as well as the extent and the duration of the transfer of rights per mode of exploitation[201]. The transfer of the rights for modes of exploitation still unknown is null and void. The licencee is obliged to actually exploit the work in good faith and in accordance with fair trade practices. A license on works still to be created must state the genre of the works and is only allowed for a limited period.[202]

There are more flexible arrangements for works created as part of an employment contract or an appointment of a civil servant. The relaxation applies exclusively for works created in the execution of the employment contract or appointment. Moreover, the employment contract or appointment must expressly provide for the transfer of copyrights. Insofar as these conditions are fulfilled, the transfer may relate to future works and modes of exploitation unknown when the employee was hired. This last case must be stipulated explicitely in the labor agreement or appointment and a share in the profit derived from the exploitation of these works must be accorded to the author. The obligation to elaborate the conditions per mode of exploitation and the obligation to exploit the work do not apply. The transfer of copyrights can be the subject of a collective agreement[203].

A similar relaxation applies to works created to order commissioned by someone active in the non-cultural sector or in advertising, in cases where the work is intended for this activity. In this case, too, the property rights on the work to be created may be transferred in advance, including future modes of exploitation. The transfer of the rights are not presumed, but must be agreed to explicitly. The obligation to elaborate the conditions per mode of exploitation and the obligation to exploit the work do not apply.

8. SANCTIONS

The Copyright Act imposes specific sanctions to restrain copyright infringements. In the first place, these sanctions intend to punish interference with the commercial exploitation of the work by the copyright holder. In addition, the Act gives the author several means to halt this interference.

8.1. PENAL SANCTIONS

A punishable offence always presupposes a material element (the act and its consequences) and a moral element (the motivation of the perpetrator). The crime of copying includes any copyright infringement perpetrated with malicious or fraudulent intent. The same applies to the malicious or fraudulent use of an author's name or of any distinctive marks used by the author to sign his creation. Works created in this manner are considered forgeries.[204]

The material element includes any action that falls under the author's monopoly, that is performed without his consent and that is not covered by a copyright exception. Exceeding the licensing conditions is also punishable. On top of this the moral element of malicious or fraudulent intent is required. "Malicious" means that one has the intention to do harm. "Fraudulent" means that one wishes to make a profit from the infringement or that one seeks an illicit advantage by fraudulently infringing upon another's rights[205]. In a commercial context, nearly every copyright infringement perpetrated knowingly and willingly is seen as fraudulent.

It is highly doubtful whether inclusion of a work in an internal business archive could be branded malicious and fraudulent. The degree to which the normal exploitation by the copyright owner is disturbed is indicative here. A work that is created by an employee and is not independently exploited will be regarded differently from a work originating from a competitor. Granting access to the work on a more or less broad scale is a more sensitive matter. The distribution of the work could seriously threaten the exploitation by the copyright holder.

In accordance with the general rules of criminal law, prosecution of accessories is possible and all forged works as well as resources used can be confiscated[206]. The penalty for forgery is a fine between 100 and 100,000 EUR, multiplied by a factor of five[207]. Beside this the judge can order the publication of the verdict. If the offence is repeated, the judge can also pass a prison sentence and order the temporary or definitive closure of the perpetrator's establishment (company, organization, …). Any interested third party may lodge a complaint; in addition to the author, this can be anyone who exploits a part of the rights. The district attorney may prosecute independently.

8.2. CIVIL SANCTIONS

The copyright owner can enter a claim for damages for copyright infringement based on the general liability rules in the Belgian Code of Civil Law. To do this, three things must be proven: wrongful act, harm and the causal connection between the two. A breach of the copyright provisions is already an wrongful act. Malicious intent or fraudulent purpose is not required: even someone who infringes a copyright in good faith can still be held liable. The harm can take various forms including lost profit and moral harm will be cited frequently. Judges often measure harm based upon the rates used by copyright collecting societies or those customary in the relevant industry. Case law recognizes the causal relationship between the copyright infringement and the harm suffered fairly easily, especially in a commercial context.

In exceptional cases, the nature of the copyright infringement is such that awarding even a minimal amount of damages is disproportionate. Sometimes bringing suit is an exaggerated measure. In such cases, the person who is strictly speaking committing a copyright infringement can counterclaim that the author is abusing the rights granted by copyright law. This could also be invoked against an employee who refuses to give permission to include his/her business correspondence and documents in the archives.

The Judicial Code contains several special procedures to help an author defend his rights. The seizure of forgeries allows the author to gather evidence of the infringement[208]. The Copyright Act provides the author with two ways to protect his rights: the author can enter a petition for injunctive relief[209] and can demand that certain materials be confiscated[210].

9. SPECIAL PROTECTION FOR COMPUTER PROGRAMS

Copyright protection for computer programs is regulated in the law of 30 June 1994 on the legal protection of computer programs. A few particularities of this law will be discussed in what follows.

9.1. DEFINITION OF THE TERM "COMPUTER PROGRAM"

No definition of the term "computer program" is provided in the law. The legislator feared that any definition would become obsolete too quickly. The preparatory texts for the EU software directive described computer programs as a set of instructions expressed in any form, language, notation or code, the purpose of which is to cause a computer to execute a particular task or function[211]. Thus on the one hand computer programs are a kind of text, and on the other hand it encompasses a set of instructions. In addition, the law points out that the preparatory material also falls within the scope of the law.

Computer programs are equated to literary works in the eyes of copyright law. The general criteria – originality and form – also apply. A program's originality must be sought in the structure used and the way in which instructions are expressed. Most programs are only distributed in binary form so that only computers can read them. The user is therefor unable to evaluate the originality and will have consider each program as potentially covered by copyright.

9.2. THE COPYRIGHT HOLDER

For computer programs, too, the initial author is the person who created the program. This rule is however mitigated in favor of employers. Only the employer is considered to be the holder of the property rights to a computer program written by one or more employees or civil servants in the execution of their tasks or at the request of the employer, unless the contract or appointment states otherwise.

9.3. EXTENT OF THE PROTECTION

A computer program is protected by the same property rights as any other work, but the moral rights are more limited. The author of a computer program has no right of divulgation, but does have the right to be credited with the authorship and the right to forbid any modification of his/her work to the extent that this would damage his honor or his reputation.

9.4. COPYRIGHT EXCEPTIONS

The author's exclusive rights are so extensive that normal use of his programs is forbidden, unless the author gives his express consent. Of course, this is not the intention of the copyright law. In order to strike a just balance, several specific exceptions have been introduced in favor of the legitimate user. This is any person who is in possession of a legally obtained copy of the program.

First and foremost, the legitimate user may use the program for the purpose for which it was created. The user may make copies, modifications and may correct any errors that may be present without the author's permission insofar as this is strictly necessary to work with his/her copy of the program.

In practice, these copies refer to the copies that the computer loads into the working memory when it runs a program. The users' agreement may impose restrictive conditions, but, of course, it cannot forbid the loading and running of the program in the working memory. The contract may not forbid the correction of errors, since such errors can hinder normal use. And the legitimate user may make one single backup copy of the program. He may not pass this backup on to another user, because it would then no longer be a backup. A backup may only be made when this is necessary for using the program. When the manufacturer provides a backup, it is generally no longer necessary to make one. When the license to use the program terminates, the right to keep a backup also ends.

It is permitted to decompile programs to the extent that this is strictly necessary to create compatible or interoperable programs. Decompiling to create a program with the same capability is excluded. This exception excludes decompiling the program to preserve it so that it can be recompiled for use on future systems.

As far as the copyright law on computer programs is concerned, the preservation of computer programs in an archive is only possible with the author's consent.

9.5. PENAL SANCTIONS

There is an additional offence relating to computer programs: putting a copy of a computer program on the market or possessing a copy for commercial reasons whilst one knows or could reasonably know that the copy is illegitimate[212].

This provision is broader than the offences described in the Copyright Act. A copy of a computer program can be a material copy (CD-ROM) or an immaterial copy (on a website). In addition to commercializing illegal copies, distributing them without a commercial objective is also punishable. This also covers free, online distribution of a copy. Reasonably knowing is a considerably weaker condition than knowingly and willingly. The penalty is a fine between 100 and 100,000 EUR, multiplied by a factor of five[213].

Including a computer program in the archive does not constitute this criminal offence. Making it available to, or allowing it to be consulted by, employees and third parties could be construed as illegal trade.

10. SPECIAL PROTECTION FOR DATABASES

Databases are protected in two different ways. The database as a whole can be protected by copyright if it is original. Both original and non-original databases fall under a *sui generis* database right, which assigns exclusive rights to the database producer.

10.1. DEFINITION OF THE TERM "DATABASE"

A "database" is a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. A database can contain copyrighted works, but it can also contain unprotected works or even raw data. The elements must be independent and may not simply be subordinate elements of a larger whole, such as, for instance, chapters in a book. A random collection of elements is not a database, but as soon as the data are ordered in any way, they satisfy the condition of systematic or methodical ordering. The user must be able to browse the various elements without having to read through the whole collection each time. This can be done by ordering the elements or setting up a search system. A database can exist in paper or electronic form[214].

10.2. HOLDER OF THE COPYRIGHT AND THE SUI GENERIS DATABASE RIGHT

The general copyright rule also applies to databases: the author is the one who created the database. For one category of databases the law presupposes that only the employer is the owner of the economic rights. This is the case when the database was developed by one or more employees or civil servants when performing their duties or following instructions from their employer, as long as the database does not belong to the cultural sector or the employer's contract or the civil servant's appointment does not state otherwise. Collective labor agreements can stipulate further details. The law does not define the term "cultural sector", which means that the courts will have to interpret this concept.

The *Sui generis* database right does not protect the intimate bond between an author and his creation, but does protect the investment made by the producer of the database. The producer is the one who took the initiative and bears the risk of the investment leading to the creation of the database[215]. Only producers established in a EU Member State enjoy the right to this protection[216]. Producers from other countries can obtain the same protection when there is an agreement on this matter between the EU and the country in question. Such agreements can only be entered into with countries offering comparable protection. Thus far, few countries have such a law.

10.3. EXTENT OF THE COPYRIGHT PROTECTION

The special regime for databases applies to the database as a whole and does not cover the elements included in it. The "database as a whole", meaning the database's structure and presentation, can enjoy copyright protection when the general conditions have been satisfied. The selection or ordering of the database's content can demonstrate its originality. However, the value of many databases lies in their completeness and functionality, two characteristics that often exclude originality. For instance, the phone book is always ordered alphabetically because a more original order would not be very practical. The general rules governing copyright apply to the elements in the database.

The author of an original database receives the same property rights to his work as is the case for other works, namely the exclusive rights of reproduction and communication.

10.4. EXTENT OF THE SUI GENERIS DATABASE RIGHT

The *sui generis* database right sets other criteria than copyright law to determine which databases fall under this regime. Databases are protected when the obtaining, verification or presentation of the contents required a substantial investment in a qualitative or quantitative sense[217]. The required investment can be a monetary investment or an investment of time or effort. Only a substantial investment is taken into account. "Substantial" can refer to a large quantitative investment or an important qualitative investment. The producer must be able to demonstrate that these conditions have been fulfilled.

The objective of the *sui generis* database right is to protect the producer's investment by granting him an exclusive right to the exploitation of the database. More specifically, the producer may impose restrictions on the retrieval and reuse of the database: "Extraction" is permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form[218]. "Re-utilization" is any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission[219].

The producer can forbid the extraction or re-utilization of the database as a whole or of a substantial part of it. The criterion "substantial part" must be evaluated relatively and is proportionate to the damage done to the producer's investment. A part can be substantial because of the amount of information (quantitative criterion) or because of the nature of the data (qualitative criterion) that is extracted or re-utilized. In some cases, the producer may also forbid the extraction or re-utilization of a non-substantial part, namely when this conflicts with the normal exploitation of the database or when this would unreasonably prejudice the legitmate interests of the producer[220].

The records manager will frequently have to archive complete databases. In that case, there is a question of extracting the database as a whole. In principle, the producer must give his/her permission for this. Making the database available to the public can then be a type of re-utilization.

10.5. SANCTIONS

A violation of the copyright on a database is punished in accordance with the general rules of the Copyright Act. The Belgian Database Protection Act creates several sanctions to protect the *sui generis* database right, which run parallel to the sanctions in the Copyright Act. Three types of actions are considered forgery[221]: the malicious or fraudulent violation of the producer's right, the malicious or fraudulent use of the producer's name or of a distinctive characteristic with which he signs his property (e.g. a logo), and finally re-utilizing copied databases for commercial purposes, storing them for re-utilization or importing them in Belgium, to the extent that the perpetrator knows that the databases have been copied.

The penalty is identical to that set by copyright law[222]. The judge can also order the publication of the verdict and the closure of the perpetrator's establishment[223]. The owner can invoke the same civil sanctions and measures as apply under copyright law. The comments on the sanctions under copyright law apply equally to this context[224].

11. CASE STUDY: ARCHIVING THE COMPANY WEBSITE

Whereas copyright has little impact on a company's paper archive, it must be given due consideration when establishing a digital archive. The inclusion of a document in the archive requires the creation of various copies. Moreover, these copies must generally be modified in order to be suitable for archiving. Granting employees access to the archive is a kind of communication to the public, even though this may be an extremely limited public. All these actions fall under the copyright holder's monopoly.

The impact of copyright law on the digital archive and the options open to the archivist are explained below by way of a practical example, more specifically archiving a company website. Organizations may wish to archive their websites for evidence purposes, for instance, in order to demonstrate compliance with disclosure requirements imposed by law.

11.1. CREATING A CORPORATE WEBSITE

In general, a website is not created by one person, but by a whole team. A graphics designer designs a logo and the style for the website. A web developer transforms this design into a usable template. A photographer provides pictures. All these elements taken separately are generally sufficiently original to be protected by copyright. The graphics designer, web developer and photographer are the original authors of these works. The whole composed by these elements produces the site's look and feel, which can be protected as a composite work.

The content of a corporate site is often provided by the marketing department. Other documents may also be published on the site, for instance, product documentation, reports or annual accounts. These documents fall under the copyright law, unless they cannot be considered original. The respective authors of these texts are the original holders of the copyright.

11.2. ARCHIVING THE COMPANY WEBSITE

There are various strategies for archiving websites. One possible option is to make a copy of all the files that were used to construct the site. Often certain changes must be made to preserve the site in way that will keep it accessible.

For dynamic websites driven by a database this may be too complicated or too expensive. In this case a screen capture movie can be made which shows how visitors view the site.

In both cases a copy of the site is produced for archival purposes. The screen capture can even be seen as a derivative work. Hence, the permission of all involved copyright holders is necessary in order to archive the site.

11.3. ARCHIVAL LICENSE

While archives and libraries in the public sector can invoke certain copyright exceptions, this is not the case in the private sector. Companies must obtain the necessary licenses to construct and use their archive. A specific archival license or a general transfer of copyrights are two possible avenues.

The company can opt to enter into a specific archival license agreement with all those involved in constructing the site. A non-transferable and non-exclusive license with the following rights can suffice: the right to make copies, to make technically necessary modifications and to make the work available within the company. With such a license, the company can manage an archive for its own internal use.

Normally, a company will wish broader rights. With respect to the contribution of the employees, in this example the marketing and production departments, the labor agreement or a CLA can stipulate the transfer of copyrights. In this way, the company acquires the property rights to all the work created by the employee in execution of his contract from the time of hiring or the closing of the CLA.

The contract with the graphics designer and the web designer can also stipulate the transfer of the property rights on works to be created. A company archive in the cultural sector is subject to more restrictive general rules rather than the more flexible rules, so that future modes of exploitation cannot be transferred.

When the photographer does not deliver made-to-order work, a license agreement must be concluded with him/her in accordance with the general rules of copyright law. The license can only cover existing modes of exploitation and must describe the conditions for each mode in detail.

A third possibility consists in requesting the respective authors to release their work under a standard open source license. The General Public License (GPL) and the Lesser General Public License (LGPL) are common examples for computer programs[225]. The various Creative Commons Public Licenses are often used for texts, music and images[226]. One characteristic of these licenses is that the author gives a non-exclusive and generally transferable license to copy, distribute and create derived products from his work. In some cases stringent reciprocity requirements apply[224].

12. ARCHIVING IS COPYING

Copyright law provides far-reaching protection for the author's interests, while the rightful interests of the user are dealt with only marginally. Archiving electronic works requires various actions that fall within the monopoly of the author. In principle, organizations must obtain permission from the copyright holders if they wish to archive protected works. With respect to copyright-protected works created by the organization's employees or to order, it is advisable to negotiate consent for archiving as early as possible.

K. CONCLUSION

The law has a profound impact on the creation, the maintenance and the use of digital archives. Many regulations exist prescribing in which form documents should be drafted and preserved. Over the past years, several obligations to use paper have been amended in favor of more technologically neutral provisions. The general rules of evidence, which indicate how documents should be created and preserved when no specific rules apply, have also been modified to better accommodate digital documents. The introduction of the electronic signature for the conclusion of contracts is an important step forward in this respect, though it is by no means the last. In general, the modernized rules leave much freedom of choice to citizens and organizations on how to design and organize their records management. The bottom line remains the ability to convince business partners, government administrations and judges of the authenticity of the documents preserved.

The preservation of digital records and the management of the archives in the private sector must comply with the legal framework on privacy protection and copyright law.

In order to achieve this, a thorough understanding is required of the source of each document, its type of content, the people involved in it and the context in which it was created. Metadata should be kept specifying which actions were performed to comply with the law.

A carefully drafted archival policy will allow organizations to control and access internal information more efficiently, while preserving reliable evidence in compliance with legal requirements. Clearly, digital archival cannot be an afterthought of information management, but should be taken into account at the design stage of any information system.

L. ANNEX 1. THE DIGITAL SIGNATURE TECHNOLOGY

Various techniques can be used to produce an electronic signature. The most widespread technology today is the digital signature. This technology served as a model for the term "advanced electronic signature" in the EU Electronic Signature Directive. The basic principles of how a digital signature works are explained in the following paragraphs.

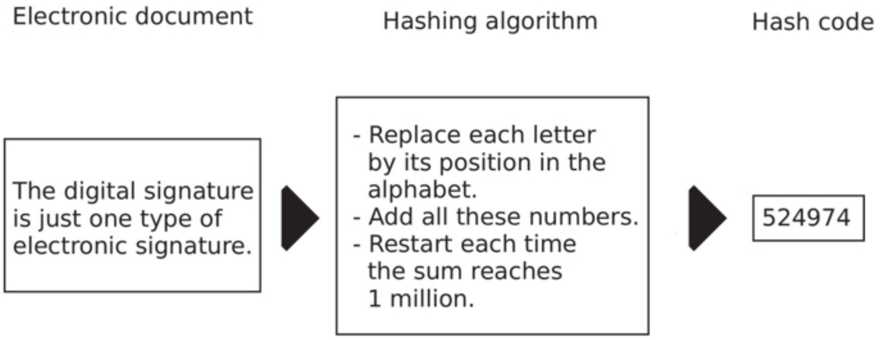
The digital signature allows two objectives to be achieved: establishing the origin of a document and verifying its integrity. These two characteristics allow the author to authenticate documents, which means that signatory confirms that he is the author of this particular document. This is also the main objective of the handwritten signature, which explains the popularity of digital signature technology among legal scholars. When exchanging information via open networks, such as the internet, such authentication can be very important.

The digital signature is a small, encrypted computer file (data in electronic form) that is added to the electronic information to be authenticated. This computer file is obtained by performing two operations on the electronic information: hashing and encrypting.

1. HASHING

Hashing is a technique with which electronic information can be reduced to a unique fixed-length code. By applying various mathematical functions to the document, the hashing algorithm calculates a hashing code. This hashing code is unique for each document, which is why it is also called a digital fingerprint. If even a single character in the digital document is modified in transmission or storage, the resulting hashing code will be different. By comparing the original hashing code with the current one, one can determine whether a document has changed or not.

A simple example can illustrate this. A simple hashing algorithm could work as follows:"replace each letter by its position in the alphabet and then add all these numbers. Restart counting at zero each time the sum of these numbers reaches one million." The end result will be a number smaller than one million. That number is the hashing code. If even one letter in the text of the message changes, then the hashing code will be different.


Electronic document
Hashing algorithm
Hash code
The digital signature is just one type of electronic signature.
- Replace each letter by its position in the alphabet.
- Add all these numbers.
- Restart each time the sum reaches 1 million.
524974

Of course, this hashing algorithm is too simple to offer certainty. If two letters or words change place, this will still produce the same hashing code. Even such a minor change could produce a new document with an entirely different meaning. The phenomenon in which two different texts produce the same hash code is called a hash collision. With a good hashing algorithm it is practically impossible, from a statistical point of view, to find two different documents with the same hashing code. Only when such an algorithm is used, can we be certain that electronic information has remained unchanged.

The original fingerprint must be safeguarded against manipulation to allow the original hashing code to be compared with the present hashing code. Encryption techniques are used to achieve this.

2. ENCRYPTION

Encryption or cryptography is the science that investigates how information can be safeguarded from, among other things, unauthorized access. In antiquity, Julius Caesar used simple encryption algorithms to exchange messages with his generals.

Encryption or encoding means that the original plaintext message is transformed into a cipher text that seams meaningless. The reverse operation is called decryption or deciphering. A key known only to the sender and recipient can be used for encrypting and decrypting. Encrypting the content of a message prevents others than the sender and recipient from being able to read it. In addition, it is certain that an encrypted message that can be deciphered by using the common secret key originates from one of these two parties. This system, in which one secret key is shared by the two parties, is called symmetric cryptography.

However, there are many disadvantages to symmetric cryptography. It is not suitable to secure electronic communication in an open network environment such as the internet. The parties to the communication must contact one another via a secure channel to exchange the secret key. However, electronic commerce will usually take place between parties who do not know or trust each other and who have only one commercial contact. During this exchange, a third party can also intercept the secret key. Moreover, this still leaves two parties holding the secret key, which means that one of the partners can pass himself off as the other. Because the same key is shared, it is still not possible to be completely sure about the sender's identity. Finally, there are an infinite number of potential sender and recipient pairs on the internet and each sender would need a separate secret key for each recipient.

Asymmetric cryptography resolves this problem by using two different but complementary keys[228]. Messages encrypted with one key – the secret key – can only be decrypted with the complementary key – the public key. The sender need only keep his key secret to be sure that no one else can send messages in his name. This can be compared with the PIN code on a bankcard. The public key may be known to all and can, for instance, be included in an electronic directory containing all the public keys for participants in the network.

In asymmetric cryptography the keys can usually also be used in reverse. A message encoded with the recipient's public key can only be deciphered with the corresponding private key. Everyone can encode messages in this manner, but only the owner of the private key can decode them. This ensures the confidentiality of the messages. This is the way to encode the content of electronic messages with asymmetric cryptography:

1. The sender looks up the recipient's public key in the electronic directory and uses this public key to encrypt the message.
2. Only the recipient can decipher the message, because no one else holds the private key corresponding to the public key that was used.

The public and private keys comprise a "key *pair*". Each participant in the network must only have one key pair to send authenticated messages and receive confidential messages. The participant can use the same key pair repeatedly, regardless of the other party with whom he/she communicates.

Asymmetric cryptography was originally developed as a new way of encrypting electronic messages so that no one besides the intended recipient could read them.

As time went by, it appeared that the reverse direction had advantageous applications. The sender can unequivocally identify himself/herself as the author of his/her messages by encrypting them with his/her private key. Everyone can use the public key to verify the origin and integrity of the messages. These characteristics make asymmetric cryptography an excellent electronic substitute for the handwritten signature.

3. SIGNING A MESSAGE

A digital signature is created as follows:

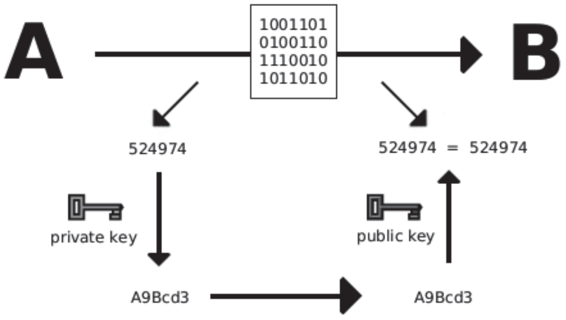
- A hashing algorithm is used to calculate the fingerprint of the message to be signed.
- Then the sender encrypts the hashing code with his own private key. The result of this process is called the "digital signature". The digital signature is added to the document and sent with it to the recipient.

It is not necessary to encrypt the complete message. Only the hashing code need be encrypted, which requires much less calculating power.

4. VERIFYING THE SIGNATURE

The recipient must verify the sender's digital signature to determine the originator of the document. This is how it is done:

- The recipient calculates the hashing code for the message received. The digital signature sent with the document is an encrypted hashing code that the sender calculated.
- The recipient looks up the sender's public key in an electronic directory or obtains it in some other way.
- The digital signature can be decoded using the public key so that the original hashing code becomes legible. The digital signature is successfully verified when the original hashing code and the calculated hashing code are identical. The recipient can then be certain about the integrity of the message. Beside this the recipient has relative certainty about the sender's identity. The message is sent by the owner of the private key that corresponds to the public key used. The sender is identified to the extent that the recipient knows with certainty who the owner of this key pair is.



Asymmetric cryptography: verification

5. PUBLIC KEY INFRASTRUCTURE

The digital signature identifies the sender of a message only relatively. The recipient must learn in one way or another who owns the public key used to verify the signature. Someone might generate a key pair and place the public key in the electronic directory under someone else's name. In this way he can pretend to be another person. There is no intrinsic bond between a key pair and a specific person.

"Certificates" explicitly establishing the link between a public key and a particular person are used to resolve this problem. A certificate can be compared with an identity card. In principle anyone can hand out such certificates stating the link between a public key and a specific person in a document, which he then signs. Third parties will consider such a certificate credible to the extent that they have confidence that the certificate issuer is telling the truth. This solution is sufficient within small circles, but it is not practicable on a large scale. That is why specialized companies offer their services as independent "trusted third parties" (TTP) that grant certificates to anyone who asks for them. These companies are called "Certificate Authorities" (CA), even though they are often private companies[229]. In this case, too, third parties will only have confidence in the certificates when they have confidence in the quality of the CA.

The CA establishes the link between a person and a public key in a certificate. Organizations as well as natural persons can own a public key. Depending on the desired level of certificate security, the CA verifies the accuracy of the identification data supplied with more or less scrutiny. A low level certificate may mention only a pseudonym. To obtain an advanced certificate, the CA can require the owner of the public key to present himself/herself in person before the certificate is issued. A certificate is no more than a digital document that is signed by the CA and that contains a public key and some identification data about the certificate holder. The link between the owner and his/her private key need not be established in a certificate, since the private key is inseparable from the public key.

The certificate holder can include a copy of the certificate with his digitally signed messages. The recipient of the digital information can verify the certificate using the CA's public key, just as the digital signature is verified using the certificate holder's public key. For this reason, the CA's public key must be disclosed. It allows the recipient to be certain which CA issued the certificate. When he trusts the CA, he will accept the link between the public key and the identity as it is established in the certificate issued by the CA

It is clear that a whole infrastructure in addition to the key pairs is needed to ensure authentication in an electronic environment. This framework, called "Public Key Infrastructure" (PKI), which consists of a combination of hardware, software and procedures, is a framework within which a variety of services based on public key cryptography can be implemented. It offers solutions for matters such as key management, certificate management, access to registers, etc. PKI is an important element in the security of the ICT environment.

A. INTRODUCTION

The DAVID-project examined how electronic records can be archived in a durable and reliable way. Long-term archiving of electronic records is a challenge for a variety of reasons and has a number of obstacles to overcome. These will be summarised one-by-one below, so it gets clear what solutions are needed for electronic record keeping. Since the DAVID-research primarily focussed on electronic records, it is useful to examine our study object more closely in the second section of this chapter. This is the initial concept from which the broad range of problems and issues is approached, which concern electronic archiving in general (section 3).

1. PROBLEMS AND ISSUES?

Administrative staff members, public servants, IT managers, records managers and archivists are increasingly confronted with the safekeeping and archiving of electronic records. Electronic record keeping is not self-evident; it requires a number of special solutions for:

- 1.1. the technological obsolescence
- 1.2. the large quantity of documents
- 1.3. the appraisal and selection process
- 1.4. the variety of documents
- 1.5. the authenticity and reliability of records
- 1.6. the archiving of the context
- 1.7. the retrieval and the accessibility

1.1. THE TECHNOLOGICAL OBSOLESCENCE

Electronic records are per definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hard- and software configurations in which they were created or managed, therefore a solution for technological obsolescence must be available. An electronic record can, after all, have a very long or even permanent archival value, while the average IT infrastructure only has an average operating lifespan between 5 and 10 years. Technological obsolescence applies also to the storage media that contains the digital information. Digital media, such as hard disks, CD-r's and tapes have a shorter operating life than traditional information carriers, such as parchment, paper or microfilm.

1.2. THE LARGE QUANTITY OF DOCUMENTS

Agencies are making full use of IT facilities for the creation and exchange of documents. The quantity of digital documents is increasing every day. Even when archival services apply the principles of appraisal and selection extremely well, they will nevertheless be confronted with a very large influx of digital documents. Appropriate solutions, such as automated archival functionalities and batch processing will be required. Such processes, however, must be controlled very precisely. Strict quality checks and error detection, as well as error correction mechanisms will be required.

1.3. THE APPRAISAL AND SELECTION PROCESS

Electronic records require hardly any physical space for their storage. Consequently one can wonder whether appraisal and selection of documents is actually still necessary, and why all digital documents cannot be archived. After all, storage continues to become cheaper all the time. Nevertheless, appraisal and selection remain necessary. Good records management demands that documents without archival value are destroyed. Digital archiving is, after all, a complex problem that requires extensive research, time and resources. These should preferably be used for documents that have the status of records. It makes no sense to store documents that have no archival value, or to demand additional transactions from users or special requirements from information systems, in which no records are produced. After all, in contrast to storage, substantial resources and efforts are required for the creation of digital documents of high-quality, which can be easily archived and conceptually managed, while maintaining their readability and accessibility. Appraisal is the key for archiving electronic records that have been created in complex and technology-dependent systems. Appraisal also plays a role in the choice of certain file formats as an archiving file format. By destroying documents without archival value, one increases the accessibility of those documents that have such value. Appraisal and selection make a more efficient records management possible. And finally, the selection also maintains control over the functional requirements for the infrastructure of electronic records management system and the digital repository.

1.4. THE VARIETY OF DOCUMENTS

The digital documents that are currently being created and received, are of a highly diverse nature. There is not only a high diversity of digital object types (word processing files, spreadsheets, e-mails, databases, images, audio visual materials, websites, GIS, CAD, virtual models, etc.), also the hard- and software configurations vary greatly. An appropriate archiving solution is necessary for each electronic record. This is not self-evident, if one takes into account the great diversity in operating systems and applications.

1.5. THE AUTHENTICITY AND RELIABILITY OF RECORDS

Digital documents have the advantage that they can always be changed after their creation. They can be modified very quickly. But, the contents of records must be fixed and unalterable. In many cases, a change in a digital document can not be detected afterwards. This can lead to doubts about the reliability, and that is why appropriate measures are required. The archivist must assure that electronic records cannot be changed without authorisation, and that eventual manipulations can be traced and be undone. This is the only way an archivist can assure the trustworthiness of electronic records.

1.6. THE ARCHIVING OF THE CONTEXT

Digital documents can only be used in the future, when the user can interpret them. In other words, the users of the electronic record must know in which context the documents were created or received and what the function and purpose of the record was. At a minimum, the users must know within which business processes the document was created, to which file or subject the document refers, and what the relation with other documents is. In the paper world, the document management and the business processes are more closely linked to one another. This link is likely to be lost in a digital environment.

1.7. THE RETRIEVAL AND THE ACCESSIBILITY

Records must be stored in a structured and accessible way to enable them to fulfil their function. This requirement is therefore also applicable to electronic records. Electronic records must be stored in a logical, well-organised and structured way, to ensure quick retrieval and preservation in relation with their context. As part of this, information about the context must be communicated to the user of the archive, so that he can fully understand the nature of the preserved records. Interpretation of electronic records is only possible if they are renderable and, as a consequence, when a solution for the problem of digital durability can be provided.

2. THE ELECTRONIC RECORD

Electronic records differ in several respects from paper records. A number of important differences are a consequence of the fact that electronic records are digital objects[1]:

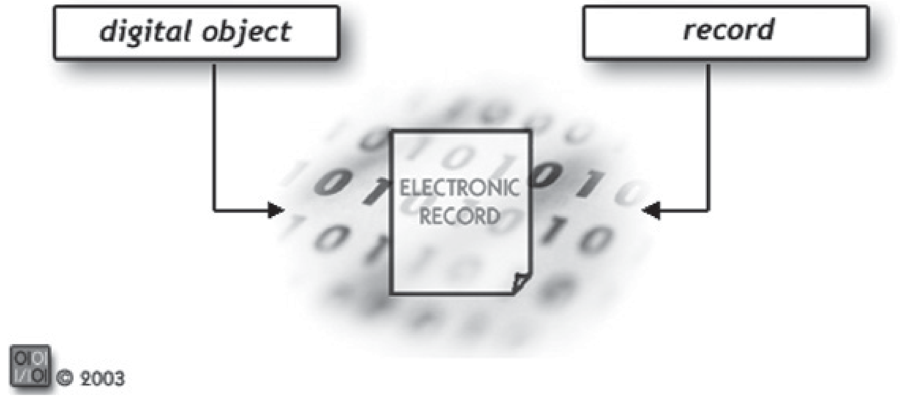
- the way in which a digital object is stored and displayed is not the same: on a digital medium, information is stored in bits (sequences of zeros and ones), while the document is displayed on screen in its conceptual documentary form. Therefore a more explicit identification and description of each electronic record is necessary.
- the storage medium and the archived record are no longer an unity: changes are no longer visually detectable.
- hard- and software are required for the rendition of a digital object: software is required for converting the bits and bytes of an electronic record (the digital representation of a record) into the documentary form of the record (the conceptual object). Digital objects can only be consulted, when the required computer equipment and software are available.
- the original bitstream cannot be differentiated from the copied bitstream.
- digital objects have different appearances: the rendering on screen of a digital document depends on the computerconfiguration and the user settings.

The look and feel of the same record isn’t always the same.

- an electronic record can also have different bit representations: the same record (for instance an e-mail message) can be stored in different formats (for instance MSG, ASCII/Unicode, TIFF, PDF, XML, etc.) and therefore in different bitstreams.
- there is no fixed relationship between electronic records and computer files, therefore making a clear identification necessary. The relationship between electronic records and computer files can be:
    - one-to-one: 1 electronic record is stored in one computer file
    - one-to-many: 1 electronic record consists of several computer files
    - many-to-one: several electronic records are stored in a single computer file.

These characteristics are inherent to the “digital nature” of electronic records. The “digital nature” is an essential characteristic of the electronic records that may not be lost, and which must also be transmitted in time. After all, archivists do depart from the archiving principle that records are archived in their primary form: what has been created in a digital way, must be archived digitally.

Through its digital properties, the concept of “the” original record is compromised. After all, the original does not survive in a digital world. The original is doomed to disappear, if only through technological obsolescence. Actually, everytime a digital document is reconstructed, a new copy of the original is created. The rendering on screen of the same bitstream will be given a new representation, depending on the computerconfiguration and the user settings. Furthermore, the original digital document cannot always be defined easily: digital documents do not have a fixed appearance or sometimes even documentary form. This makes it even more difficult to define the original “look and feel” of a document. Finally, the original bitstreams and their copies cannot be differentiated from one another.



Electronic records are, on the other hand, also more than just digital objects. Electronic records inherit characteristics from their recordness. Electronic records are differentiated from digital objects and digital information by their[2]:

- fixed documentary form[3]: the structure, the composition and the defined rendering of the document
- a static or a fixed content ("capture")
- context: the archival bond with the records creator, with the business process in which they were created or received, together with related records.

In general, five components are differentiated in an electronic record[4]:

- content
- structure
- context
- layout, "look and feel"
- behaviour, functionality.

The identification of the records, and the appraisal, results in a definition of the essential and incidental properties or components of a record. The content, the structure and the context of the record are essential components[5]. By contrast, the "look and feel" and the behaviour are not always essential for the recordness of documents. These composing parts are not always equally easy to archive. The "look and feel" and the behaviour are often so dependent on a specific computer application that it is barely possible or even impossible to store them without these programs.

The essential properties must be archived in an unaltered way, while the incidental properties may be lost or changed. InterPARES research has shown that a record keeping procedure for authentic records does not mean that the electronic records may not be subjected to any changes, but that the final purpose of the document may not have been changed and that the essential components are complete and correct.[6]

3. DIGITAL ARCHIVING

The goal of digital archiving is to transmit an interpretable electronic record over time. It is best to proceed from the assumption that the receiver of the electronic record must have access to the conceptual document stored in the computerfile, and that this document must be understandable. This implies, that both the future computer and the future user must be capable of processing the preserved bits and of understanding the electronic records. This leads to three requirements that must be met by electronic records. They need to be executable, renderable and understandable:

- executable: the digital storage media must contain intact bitstreams and it must be possible to transfer these to the computermemory
- renderable: the bitstreams must be processed correctly by the computer, so that the record can be displayed on screen

- understandable: the user knows the function, the meaning and the context of the record, making the records re-usable.

The preceding shows that the mere storage of bitstreams ("bit preservation") is insufficient in order to gain access to the content of electronic records. The consultation of an interpretable record is only possible, when a linked sequence of dependencies can be executed correctly:

1. the digital storage medium contains intact bitstreams
2. the bitstreams can be transfered to the computer memory. Properly functioning peripheral equipment, ports, drivers, cables and operating systems are required. The operating system of the computer must be compatible with the filesystem of the storage medium.
3. the loaded bits can be rendered as the conceptual records, and they will be displayed as such on screen. This is only possible when one disposes over the necessary application software, which supports the file format of the electronic record.
4. the user has information about the context in which the document was created or used, so that he/she can fully assess the function and the meaning of the document.

The electronic record is no longer interpretable, and it must be considered as lost or no longer usable, if any one of these sequential steps is missing. The greater the number of dependencies, the greater the risk is of losing of records. For these reasons, elements such as backup formats, compression and encryption should be avoided as much as possible.

The characteristics of an electronic record also show that digital archiving is not the same as making a backup copy. The goal of backup copies is to repair lost or deleted digital files in the short-term, while electronic records must be re-usable in the long-term. In the case of backups, the basic assumption is that the original IT configuration is still present, which will not be the case for electronic records that have a long-term archival value. Backup copies are also usually used by the authors of the documents themselves, who are capable of using these documents without additional contextual or administrative metadata. In most cases, the users of electronic records are not the authors nor one of its initial recipients.

4. CONCLUSION

Digital archiving includes:

- the preservation of the digital nature of an electronic record
- preserving the possibility of reconstructing the electronic record, i.e. making sure that electronic records can be consulted in the future
- making an interaction between the stored bitstreams, on the one hand, and a hard- and software configuration, on the other hand, possible: taking the required measures, so that usable and accessible electronic records are archived

- limiting (external) dependencies to a minimum
- risk assessment: evaluation and limitation of risks, including the deployment of security measures
- more than just saving digital objects, and therefore also:
    - defining the essential properties or components of an electronic record through a unique identification of the records and appraisal
    - explicit registration and archiving of information about the archival bond and the context: ensuring that electronic records can be understood correctly
    - transmitting knowledge in time: making the conceptual content and the meaning of an electronic records accessible
- storage with a long-term vision: electronic records can have a permanent archival value
- bringing digital documents under conceptual control and administration
- taking archiving into account, as soon as an electronic record is created or received: appropriate procedures must be embedded in the complete life-cycle of documents, including pro-active procedures to ensure the creation and management of electronic records of high quality.

B. PRESERVATION STRATEGIES

Electronic records are digital objects. Various strategies can be applied for the long-term preservation of a digital object. Below we will discuss the most common preservation strategies, and we will examine to what extent these are suitable for the long-term preservation of electronic records[7]. The following preservation strategies are discussed:

1. Hard copy strategy
2. Preservation of technology
3. Conversion
4. Migration
5. Conclusion: preservation of the original and the migrated bitstreams

1. HARD COPY STRATEGY

In the hardcopy strategy, electronic records are transferred to microfilm, or printed out on paper.

However, archival science proceeds from the principle that records should be archived in their original, primary form: what was created digitally will be archived digitally. The same holds for records created in paper form. In a conversion to paper or microfilm, an essential characteristic of a digital document is lost, namely its "digital nature". For this reason alone, the hard copy strategy is inadvisable. Furthermore, there are still some other factors that apply in a conversion to paper or microfilm:

- the records lose their "digital advantages", such as reusability, central storage and decentralised accessibility, automated composition of archival descriptions, automated queries, etc.
- some functionalities or behaviour of the electronic record may be lost
- for the destruction or replacement of a record, the approval of the Director of the National Archives or his authorised deputy is required (art. 5, Public records act of 24 June 1955)
- it is difficult to avoid that te digital versions of documents continue to be used as a basis for transactions: the familiarity with digital information is growing and the digital versions will continue to be viewed and used as the primary copy in business processes
- not all essential information is always printed out
- not all electronic records can easily be transferred to paper or microfilm (for instance GIS, CAD, multimedia objects, databases)
- higher costs: a conversion to paper and microfilm, and the storage of paper records is more expensive than digital archiving.

A printout on paper, or a transfer to microfilm, can only be considered as a temporary archiving solution, which is applied in expectation of a full electronic record keeping procedure. This option is, by the way, not applicable to all types of digital documents; only the electronic records with a paper equivalent can be printed out easily. An important requirement is that all essential information will be included on the printout or the microfilm version.

2. PRESERVATION OF TECHNOLOGY

2.1 COMPUTER MUSEUM STRATEGY

This approach consists of the storage of the original hard- and software, with which the electronic records were created or managed. In this way, an outdated computer configuration is maintained, so that the computer files can be consulted in their original form.

For medium-term and long-term storage, this solution is not feasible:

- all the various configurations must be stored
- hard- and software have a limited life-cycle
- old hardware components are becoming increasingly scarce
- the IT know-how, which is required for working with the old hard- and software, disappears
- product support becomes increasingly difficult with the passage of time
- a transfer of electronic records to new storage media becomes necessary, because of the (natural) degradation of storage media. The new storage media will probably not be compatible with the old computer configurations.

This approach is only possible for short-term storage (5 to 10 years) of electronic records. The museum strategy is therefore only usable for the storage of those records, where the archival value does not exceed the lifespan of the technology, or as a temporary solution that is applied in expectation of a more persistent record keeping solution. Old computer configurations can sometimes still be used for the recuperation of records in outdated formats.

2.2 EMULATION

In the emulation strategy, the original hard- and software is not preserved. Instead, the required platform is simulated on future (newer) computer configurations, so that electronic records can be consulted in their original (obsolete) file format.

Emulation can be applied at various levels. One can imitate the computer hardware, the operating systems, specific software or a combination of these. Emulation is possible on the basis of configurable chips (emulation via hardware), or on the basis of computer programs (emulation via software).

At the moment different views exist, with regard to the way emulation can be applied in digital archiving:

- Jeff Rothenberg: Emulation Virtual Machine[8]
- Steve Gilheany: Turing Machine[9]
- Raymond Lorie: Universal Virtual Machine (data preservation, program preservation)[10]
- Cedars & Camileon project: Migration on request[11]

Emulation has a number of interesting advantages:

- in theory, the documents can be preserved and accessed in their original format:
    - all original properties and functionalities are maintained
    - no elements are lost as a consequence of conversion or migration
    - the authenticity of the electronic records is easier to guarantee
- the formats of the stored documents do not have to be changed, every time an archiving file format becomes obsolete
- the cost is not dependant on the number of preserved electronic records.

On the other hand, there are also a number of disadvantages that are connected to emulation:

- emulation is technically very complex: the necessary know-how and expertise for developing and maintaining an emulation system is not available in archival institutions. As a consequence, the archival institutions depend on external services and partners. This is in conflict with the goal to build up a self-containing digital archive.
- emulation has high development and maintenance costs: will archives, which opt for this approach at the present time, have the financial means to maintain this system in the future?
- the platforms, on which these emulation programs run, evolve, which means that

a conversion or migration of the emulation programs is necessary in due time

- overkill: certain emulation approaches proceed from a complete simulation of the original applications, including all editing functionalities, while a viewer for a display of a (static) record is sufficient in principle. Emulation is directed primarily to the long-term preservation of systems and software, while the archivist is, in the first place, concerned with the digital archiving of records.
- creators utilise a large variety of different information systems, a number of which have been specifically developed for the organisation or were programmed on an ad hoc basis. Archival services must have a large number of emulators at their disposal, and it is not possible to share some of the costs with other archives.
- the protection of author's rights on hard- and software leads to restrictions on reverse engineering, decompilation and disassembly of code, which limits the creation of emulators
- emulation of closed or undocumented file formats, which is based on reverse engineering, is risky if not impossible. Emulation of standardised or documented formats is easier and safer. Must emulation then be preceded by migration to an open archiving file format after all?
- users work with outdated software and cannot make use of technological innovations
- archives must not only maintain electronic records, but also emulation hard- and software, and the necessay documentation.
- the feasibility of certain emulation approaches will only become apparent in the future.

The most important argument that is presented by the promoters of emulation, as a digital preservation strategy, is primarily the maintenance of the original computer file, with all its original properties. One especially emphasises the possibility of storing the "look and feel" and the functionalities, while these properties are often changed or lost during conversion or migration. They do not question whether all of the "original" properties contribute to the recordness of an electronic document, or how the original "look and feel" can be defined, nor whether the maintenance of the original functionalities is really an essential condition. They view electronic records merely as digital artefacts, all of whose properties must be maintained. It is not a coincidence that the great advocates of emulation are in the first place computer scientists. One should not forget that archives have other goals than museums, and that appraisal and contextualisation are essential tasks for archivists.

Nonetheless, emulation remains a potential strategy, which may have its benefits for the long-term preservation of electronic records. In all events, the experience with emulation as a digital preservation strategy is limited at the present time. Furthermore and up to the present, very few large-scale emulation applications are operational for digital archiving purposes.

3. CONVERSION

In the case of conversion, digital documents are converted from a lower to a higher version of the same file format. An example is the conversion of a document that was created in MS Word 97 to MS Word 2000.

The advantages:

- the documents remain executable and fully functional.

The disadvantages:

- electronic records must be converted with a high-frequency (for instance MS Word 6.0 • MS Word97 • MS Word2000 • MS Word2002 • MS Word2003)
- properties are often changed or lost, which means that the authenticity of the document is more difficult to guarantee
- digital documents frequently continue to be stored in a manufacturer, software or version-dependant format: absolutely no guarantee for long-term support is available from the manufacturer of software-dependant formats.

Conversion is not a practical long-term storage strategy for digital documents. As a consequence, conversion should be avoided as much as possible, unless no other possibilities are available. For instance when no suitable archiving file format is available, or if the loss of essential components of the record appears imminent.

4. MIGRATION

Migration is a preservation strategy, in which digital documents are transformed into suitable archiving file formats. This is currently the most frequent method used for archiving electronic records.

Since suitable archiving file formats are preferably standardised file formats, this preservation strategy provides for the migration of electronic records (from a propriatary) to a standardised format. Standards are documented, stable and not dependent on one manufacturer. Migration is sometimes also indicated by the terms "transformation" or "normalisation", whenever standards are used as a target format.

The advantages of migration as a storage strategy are:

- electronic records are not stored in a manufacturer-, software- or version-dependant file format
- the specification of the file format is available: on the basis of this format documentation, a new viewer can be programmed at any time
- availability of conversion tools: besides the many conversion tools that are available on the market, migration is also easy to realise with the help of widely available computer programs.

The disadvantages:

- this storage strategy is strongly depending on standards. However, standards have a number of disadvantages:
    - their development process takes a long time; this means that standards cannot follow the speed of the market evolution
    - standards are not always precisely applied or implemented: standards are sometimes expanded, so that additional functionalities become available, through which the documents are no longer fully compatible
    - standards support almost most no application-oriented functionalities
    - not all standards are equally well distributed or have a sufficient market penetration
    - standards do not have an unlimited lifespan
- for some file formats there are no suitable archiving file formats available
- the original properties or functionalities of the source format can rarely integrally be transferred to the target format: migration is in many cases associated with loss
- at each conversion, the authenticity of the record is threatened.

Migration is at present the most frequently used strategy for the long-term preservation of electronic records. One must, however, make sure that no essential information is lost during migration, and that the authenticity of the electronic records is not compromised. In principle, this is no hindrance for the application of a migration strategy. With a thorough analysis of the source and the target format, such risks can be avoided and any losses limited to a minimum. Based on an appraisal decision, this should lead to the migration of all essential and as many of the incidental properties as possible.

The migration procedure should be automated, taking into account the large quantity of electronic records. Manual conversions are labour intensive and not always consistently accurate. Automated migration procedures lead to a number of special requirements for the migration process. One must define a migration path for each record type. A migration path consists of the following steps:

- appraisal and selection: identify the record and define the essential and incidental characteristics of the record
- choice of the target file format
    - choose a file format that fulfills the requirements of a suitable archiving file format (see C.3.2)
    - choose a file format that supports all essential components of the electronic record
    - define the profile of the target file format (uncompressed, color schema, encapsulation of metadata, etc.)
    - pay attention to the encapsulated metadata in the source files
- choice of the migration tool:
    - select a "documented" migration tool: avoid "black box" migration tools. Make sure you know which operations are performed behind the scenes
    - select a migration tool:

  - only after extensive testing
  - that leaves the source files unaltered
  - with error-handling: error-detection, error-correction and error-logging
- tests: include an extended test phase of the procedure and the transformation operation, before migration is effectively applied
- migration of the electronic records
- validation of the transformed records: check the quality of the records: verify whether the transformed records are in conformity with the specification of the archiving file format and the applied profile
- document the entire migration process

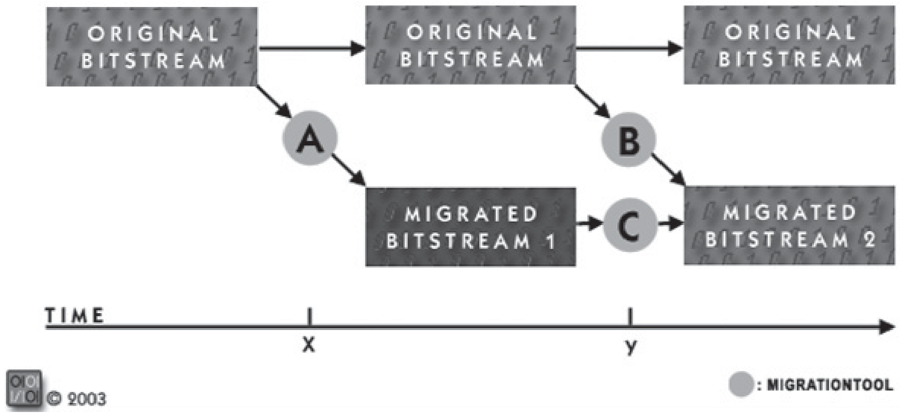
5. CONCLUSION: PRESERVATION OF THE ORIGINAL AND THE MIGRATED BITSTREAMS

An evaluation of the possible preservation strategies shows that there are currently no definitive solutions for the long-term preservation of electronic records. None of the discussed preservation strategies is free of risk.

The search for a suitable preservation strategy has for many years focused on the question, whether an emulation of the original software environment or, instead, a migration of electronic records is the best solution. Both solutions have one common denominator, namely that they translate a bitstream into a readable document. Migration and emulation, however, do this at a different point in time. With migration this is carried out in the present, while emulation projects this action somewhere in the future. Migration tackles the problem by dealing with the document side, whereas emulation searches for a solution for the readability problem on the hard- and software side.

In the meantime, the view that both approaches do not need to exclude one another has won ground. Both solutions are complimentary in the life-cycle of an electronic record, or are more suitable for a certain type of electronic records. In general, emulation is more suitable when the "look and feel" and the behaviour of the document is important, while migration is sufficient whenever the content and the structure represent the essential components of a record. For a successful emulation, the specifications of the technology must be available. A number of in between solutions also exist, which combine elements of migration and emulation.

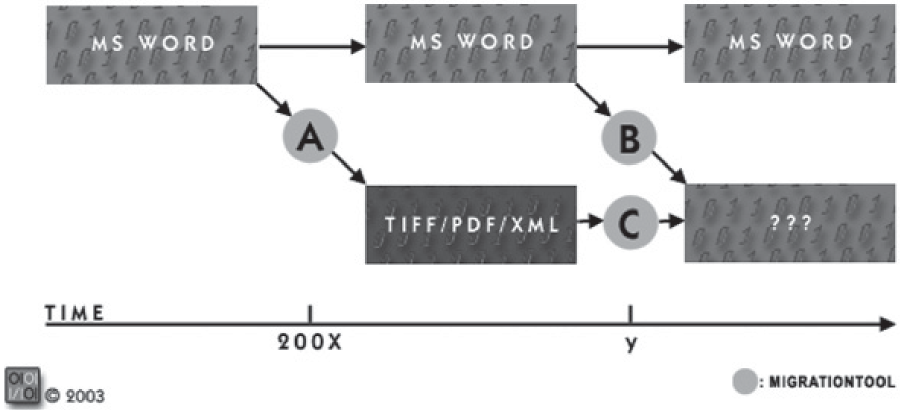
The preservation strategy that is recommended by the DAVID-project[12] is a middle way between emulation and migration, keeping all options open for the future and offering a direct solution for the readability problem. This can be achieved when we preserve the original bitstreams together with the migrated versions, which offers more quarantees towards long-term readability, of those bitstreams. Electronic records, which have not been stored in a suitable archiving file format, are migrated to a suitable archiving file format before their ingest into the digital repository. The record in its original file format is not destroyed; instead it is also included in the digital repository. This means that two bit representations of the same electronic record are preserved: one in its original file format, and one in the migrated file format. It is possible to store these representations in separate computer files, or to encapsulate them in one XML container. This offers the advantage that in the future both emulation and migration are possible, either from the original or from the migrated file format. No migration is necessary for electronic records, which were directly created in a suitable archiving file format, so only one representation of such record must be preserved.



When applied to a text document which had been saved in an MS Word file format, this preservation strategy includes the following steps. At the latest at the time the document is ingested in the digital repository (moment x), the text document in an MS Word format will be migrated to a suitable archiving file format with migration tool A. Depending on an identification of the essential components and on appraisal, a selection will be made from the XML, TIFF and PDF archiving file formats. MS Word is after all an undocumented file format that is dependant upon one manufacturer and one application, for which only time-limited support is available[13], making it totally unsuitable for long-term archiving. In the digital repository, both the original MS Word file and the migrated file are stored. Whenever the XML, TIFF or PDF archiving file formats threaten to become obsolete (moment y), one has a choice between various options:

- the use of an emulator for the MS Word format
- the use of an emulator for the migrated format
- migration to a new archiving file format (migrated bitstream 2), carried out on the MS Word file with migration tool B

- migration to a new archiving file format (migrated bitstream 2), carried out on the migrated file format (migrated bitstream 1) with migration tool C.



Even if, in the case of MS Word, emulation appears to be a relatively unlikely possibility, this preservation strategy could mean that more of the original properties of the record are preserved in the second archiving file format than in the first archiving file format.

C. *ARCHIVING STANDARDS*

1. IMPORTANCE

IT standards play an important role in every preservation strategy. In the case of migration, the record is preferably transformed to a standardised file format. This means that records do not frequently need to be migrated. Since the technical specifications of standardised file formats are available, new viewers can be programmed for the outdated format at any time. Emulation of software for the visualisation of documents in standardised file formats, is simpler and more realistic then building an emulator for undocumented or closed file formats. And finally, standards are also important for the storage of records on media. After all, digital preservation media are also subject to technological obsolescence. For the storage of records on a preservation media, physical (type of preservation media) and a logical (filesystem) standards are preferably applied, so the electronic records are at least exchangeable.

Standards can be applied to:

- the preservation media on which the electronic records are stored
- the file formats in which the electronic records are stored.

2. PRESERVATION MEDIA

2.1. DURABLE STORAGE MEDIA

Whether electronic records will still be renderable in the future depends, in the first place, on the media on which they have been stored. Electronic records are best stored on durable preservation media. The preservation media must be capable of storing data for the long-term and may not deteriorate all too quickly.

The lifespan of storage media is usually examined on the basis of tests, whereby the ageing process is speeded up and where the number of errors on the aged storage media are measured. The lifespan of the storage media is subsequently forecast on the basis of these tests, and on the assumption that the medium is stored under good conditions. An error-detection and error-correction system is taken into account in this regard. After all, an error-detection and error-correction system exists for every type of storage medium. These mechanisms can repair errors on the storage medium up to a certain level, so that the electronic files remain readable. The number of correctable errors does, however, have an upper limit. Computer files become unreadable once this threshold is exceeded. The lifespan tests give a good indication of the expected life expectancy of the storage medium, but they are in themselves no guarantee for the readability of the records in the long-term.

A durable preservation medium and good material storage conditions only assure that the storage media still contain the data that was transferred to them at one point in time. Whether the information on the storage media can effectively still be retrieved and executed depends on the available technology.

2.2. LIFE EXPECTANCY OF TECHNOLOGY

One must have access to the necessary hard- and software in the future, to be able to load the information on a certain storage medium into the computer's memory (a.o. equipment, operating systems, drivers, cables, etc.). This technology ages quickly and usually has a shorter life expectancy than the media on which the electronic records are stored. From this viewpoint, it is irrelevant whether a CD-r has a life expectancy of 100 years or not. There is a substantial probability that the equipment and/or the programs, for reading the data on a CD-r will no longer be available in 10 or 20 years[14]. At present this is already the case for a variety of diskette and tape formats. And this is valid for all types of storage media, both optical and magnetic. The lifespan of a storage media is, as a consequence, in part determined by the available technology. Transferral to other storage media will become necessary, as soon as a certain technology is likely to become unavailable. By carefully selecting a stable preservation medium and a durable technology, the frequency of refreshing operations can be reduced to a minimum.

2.3. GENERAL RECOMMENDATIONS

Both magnetic and optical storage media are, in practice, used as preservation media for electronic records. The following recommendations apply to both types of media:

- spread the risk: if possible, store the electronic records on several different types of preservation media; do maintain a close control over the number of different types of optical and digital preservation media for electronic records, so that the number of supported systems can remain limited
- opt for storage media and technology that has proven its reliability and operational safety; avoid the newest technologies that have not proven themselves in this regard
- store records on media that do not degrade too quickly: select storage media with a long life expectancy and a robust error-detection and error-correction system
- make sure that the required equipment and software applications are available:
  - physical format: use standardised storage media, which can be read by different types of equipment produced by several different manufacturers
  - logical format: Write data to the storage medium using a standardised file system
- make safety copies and store these in separate and safe locations off-site: the number of safety copies that are required increases with the capacity and density of the preservation medium
- store the storage media under good material conditions
- carry out regular quality controls
- transfer the electronic records to a new preservation media, whenever:
  - the number of correctable errors on the storage medium rises strongly
  - when the technology threatens to become obsolete
- check the integrity of the transferred bitstreams during refresh procedures (for instance by comparing checksums)
- prepare a disaster and recovery plan for every type of storage media containing electronic records
- together with each preservation medium, store an overview of the folder structure and its contents
- store the records in a standardised filesystem, using an open, documented and uncompressed file format on the storage medium.

2.4. MAGNETIC PRESERVATION MEDIA

More information and practical recommendations are available on the DAVID-website:

- Digital ArchiVing. guIdeline & aDvice, no. 6: *Durable magnetic carriers*
- F. BOUDREZ, *Magnetische dragers voor het archief*, City Archives of Antwerp, Antwerp, 2002.

Recommendation: be careful when using hard disks as a medium for long-term storage!

- use a type of hard disk that has proven its durability
- make sure that safety procedures against data loss are available (for instance RAID 5)
- hard disks are not durable; they have a relatively short life expectancy (due to heat, wear and tear)
- folders and files are saved in a filesystem that is defined by a certain type of operating system; a duplicate storage in two different types of filesystems (for instance Windows and Unix/Linux) gives extra security.

Recommendation: do not use backup tapes for archiving purposes!

Backup tapes are usually compressed copies of platform-dependent computer files. Backup tapes are worthless without the original backup software and the computer operating system, as well as the application with which the electronic records were created:

- backup formats are usually undocumented or closed formats, which are proprietory to a certain manufacturer or part of a certain backup program
- backup files are usually compressed: specific software is required for decompressing such files
- not all information that is required for the reconstruction of computer files is necessarily stored on the storage medium. Certain, essential information is maintained on a backup computer
- backup tapes serve short-term file recovery goals, and not long-term preservation of electronic records
- backup tapes do not provide (administrative or technical) metadata about the context of the records.

2.5. OPTICAL PRESERVATION MEDIA

More information and practical recommendations are available on the DAVID-website:

- Digital ArchiVing. guIdeline & aDvice, no. 2: *Durable CD's*
- F. BOUDREZ, *CDs voor het archief*, City Archives of Antwerp, Antwerp, 2001)

Recommendation: do not use DVD as a long-term preservation medium!

- the standardisation of DVD technology has not been completed yet: different standards exists besides each other.
- writable DVDs are not easily exchangeable.

3. FILE FORMATS

Electronic records are preferably stored in a standardised file format. As a rule, standardised file formats are:

- open and documented: their technical specifications are available. One can assume that viewers can easily be programmed, when the technical specification of the file format is available.
- stable: standards can only be revised when a certain procedure has been observed
- software independent: the standards are supported by the different software applications and open source initiatives
- manufacturer independent.

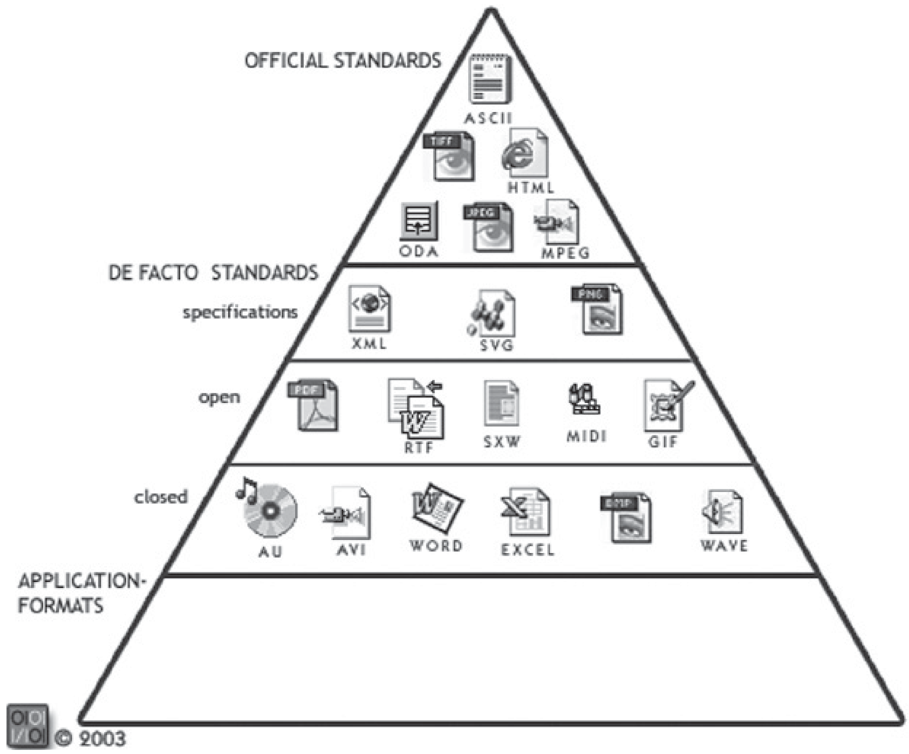
3.1. HIERARCHY

A large number of different standards exist in the IT world. A hierarchical subdivision can be used for maintaining an overview, as well as a basic principle in the choice of a certain file format for record keeping purposes.

The official standards are located at the top of this hierarchy. These standards have been defined by official standardisation organisations, and they owe their official status to the participation of a(n) (inter)governmental organisation. Well known examples are ISO (International Organisation for Standardisation), *IEC* (International Electrotechnical Commission) and *ITU* (International Telecommunications Union). Besides these, many other official regional and national standardisation organisations exist.

Below the official standards, the so-called de facto standards are situated. The group of de facto standards can be subdivided into three subgroups. The specifications are the result of non-official standardisation initiatives (for instance W3C). Their management is not in the hands of a manufacturer, but is controlled by a standardisation institute. The open formats, exactly like the specifications, are publicly documented, but their management depends on one manufacturer. And, finally, there are the closed formats. These formats can be considered as de facto standards, due to their wide distribution, but their technical specifications are not open and are managed by one manufacturer.

When selecting a suitable archiving file format, it is preferable to concentrate on official standards and specifications. A dose of pragmatism is recommended in this regard. The hierarchy is an important guideline, but it is not the be-all and end-all. The status of official standard does not in itself give any guarantee. For instance, certain specifications are more widely applied than their official equivalents (see Unicode vs. ISO-10646; XML vs. SGML). Next to the degree of standardisation, there are still other criteria that are valid for suitable archiving file formats.



3.2. SUITABLE ARCHIVING FILE FORMATS

A suitable archiving file format preferably meets the following criteria:

- standardised: documented, stable and not depending on one manufacturer
- widely distributed with sufficient market penetration
- exchangeable: independent of certain operating systems, network protocols and applications
- provides a robust error-detection and error-correction mechanism: errors in bit storage are repairable
- possibilities for systematic and automated validation
- well-structured storage of information
- storage without information loss (no *lossy* compression)
- possibility for including certain (self-defined) metadata fields
- capable of transmitting essential properties of the record over time
- protection of the authenticity of the record
- autonomous and self-containing
- possibility for media and equipment independent storage
- user-friendly.

These criteria are important in the choice of a certain file format as the archiving file format. It is also best to remember these quality requirements when applying archiving standards. Standards can, after all, be applied in various ways. Most archiving file formats make it possible for the user to define a number of settings and parameters. For instance, one can create a number of different types of TIFF, XML and PDF files, but not every TIFF, XML or PDF document is suitable for long-term preservation. JPEG compression can for instance be applied to images that are stored as TIFF files. Not only data is lost during this process, but one is also dependent on the corresponding decompression for a reconstruction. The quality of XML documents depends on the granularity, the nesting and semantics of the XML-tags. PDF documents that are destined for long-term preservation are preferably tagged, or at least structured.

It is best to keep electronic records as autonomous as possible. The dependencies for a reconstruction are preferably limited to an absolute minimum. The lack of a single necessary link in the reconstruction process can, after all, lead to the loss of the record. This is the reason why compression, encryption, passwords or other security settings should be avoided as much as possible.

More information about suitable archiving file formats is available on the DAVID-website:

- Digital ArchiVing. guIdeline & aDvice, no. 4: *Standards for file formats*
- F. BOUDREZ, *Standaarden voor digitale archiefdocumenten*, City Archives of Antwerp, Antwerp, 2002-2005.
- F. BOUDREZ, *<XML/> and electronic record keeping*, City Archives of Antwerp, Antwerp, 2002.

For certain types of digital information, no suitable archiving file formats are (as yet) available. These digital documents are so closely linked to the hard- and software environment in which they were created that they can only barely (or not at all) be used outside that environment. This is the case for certain type of multimedia objects at the present time. In such a case it is recommended to search for a file format which answers as closely as possible to the criteria of a suitable archiving file format, whereby any dependencies are avoided to a maximum degree.

Recommendation: do not use compression for long-term preservation!

The application of compression is avoided for the following reasons:

- decompression is an extra step in the reconstruction process from preserved bits to understandable document on screen, which conflicts with the principle of avoiding all possible dependencies
- information and quality is lost in the case of *lossy* compression. The loss of quality, noise and/or deformation, easily becomes audible or visually perceivable in audio-visual records, when different compression algorithms are applied in sequence
- the processing of compressed bitstreams is more complex
- compressed digital documents are more vulnerable than uncompressed documents: an error in a compressed file leads more quickly to an irretrievable loss of data
- the need for compression is usually due to technological limitations (processing, storage, transmission): these limitations will become less rigid and probably disappear entirely in the coming years, due to technological progress.

If compression is unavoidable, then one should opt for a lossless compression method (one without data loss) and select a compression method with an open, documented and standardised decompression algorithm.

3.3. EXAMPLES OF SUITABLE ARCHIVING FILE FORMATS

TYPE OF DOCUMENT	ARCHIVING FILE FORMAT
Text:	ASCII/UNICODE, TIFF, PDF, XML
Images:	
Screen	TIFF, PNG
Vector	SVG
Screen and vector	CGM
Sound:	WAV (uncompressed PCM)
CAD:	DXF
GIS:	GML
Video:	MXF

Recommendations:

- limit the number of file formats that are used within the organisation as an archiving file format
- if possible, store electronic records immediately after their creation in a suitable archiving file format
- do not preserve electronic records in a closed or undocumented format
- avoid the use of compression (for instance LZW, JPEG, ZIP in a TIFF file; ZIP in a PDF-file)
- do not wrap up records into compressed formats (.zip, .tar, .rar)
- whenever the original formats are not saved, destroy the original computer files only after the migration has been checked and validated
- check that the standards are applied correctly, and also verify that the electronic records are conform the formal definition of the standard.

D. POLICY AND PROCEDURES

1. ARCHIVING POLICY

Every organisation needs a general policy, which defines the basic options and the goal of the record keeping procedures within the organisation. This policy must make a coherent records management and record keeping possible, the final goal of which is that records are managed in a good, structured and accessible way, for as long as this is required. The archiving policy is a platform on which record management actions and record keeping procedures are implemented.

The archiving policy within an organisation is preferably defined in a policy document, which has been formally approved and which is applicable both to the paper and to the electronic records. Such a document defines, among other things:

- what the general goals and basic principles of the record keeping policy of the organisation are
- what legal obligations are applicable to the records management and record keeping procedures within the organisation
- which documents have the status of record within the organisation
- which documents are preserved on paper and which are preserved electronicly
- the long-term preservation strategy that is observed for electronic records
- how and to what degree the reliability of the electronic records is guaranteed
- which part of the organisation is mandated for developing the record keeping procedures
- how the competencies and the responsibilities are distributed between the agencies, the IT managers and the archival service
- what the general guidelines are for the creation, use, management, archiving and disposition of (electronic) records
- how the costs are divided
- what the creators and the archive users may expect.

2. THE OPEN ARCHIVAL INFORMATION SYSTEM (OAIS) MODEL

The Open Archival Information System (OAIS) model can be used as a guide in the development of an information management and record keeping system. OAIS was developed by the Consultative Committee of NASA for their Space Data Systems, and in the meantime it is established as an ISO standard (ISO-14721:2002)[15]. Although the OAIS model is applicable to both paper and electronic records, the model is primarily directed towards the second category.

The OAIS model is not a system model for a record keeping system which can be implemented immediately, it is rather a conceptual reference model. It offers a framework in which procedures for the long-term archiving of digital information can be developed. For developing a record keeping procedure, the processes and metadata that are identified within OIAS are, amongst others, important. The functions, activities and workflow are primary parts of every record keeping system, and they give form to the record keeping function of an archival institution or archival service:

- ingest: quality control, registration, description, extraction of metadata, migration of records, etc.
- long-term storage (physical management): the provision of good material

circumstances, refreshing of preservation media, error-detection (checksums), disaster plans, the preparation of backups, the maintenance of readability, etc.

- assuring accessibility (logical management): creation and updating of archival descriptions and metadata, and the provision of retrieval paths
- management: defining a policy, consultation with the archive creators, choosing standards, management of the digital repository, maintenance of documentation, follow-up on technological changes, etc.
- providing access to the archives and the records.

These five functions are the key processes in every record keeping procedure for electronic records, and they cover the entire document flow between the creator and the users of the archives. How these processes will look like, depends on the concrete design and realization of the record keeping procedures.

3. TOWARDS A CONCRETE RECORD KEEPING PROCEDURE

The record keeping policy and the archiving function within an organisation are put into practice through concrete archiving procedures.

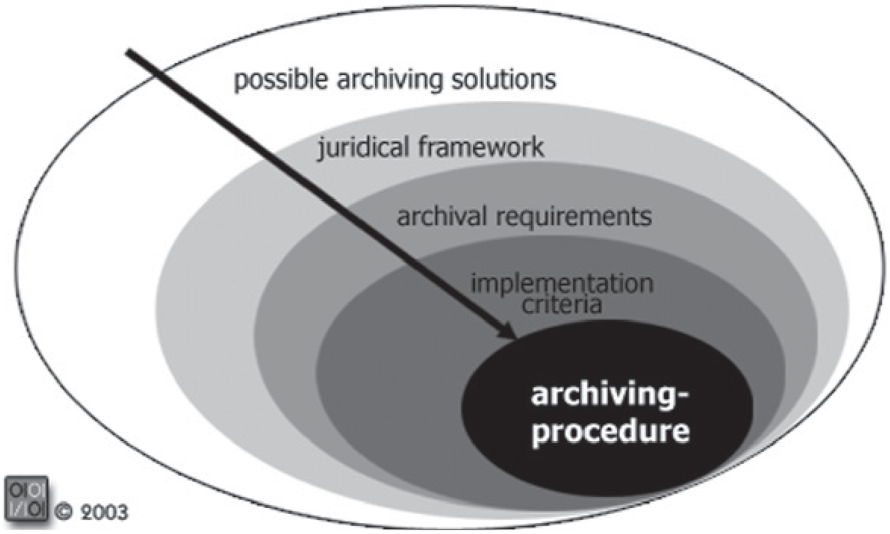
A variety of archiving procedures are applicable for the archiving of electronic records. It is important for the creator of the archive to select the archiving procedures that are most effective for the organisation and its records. Generally, the development of a good archiving procedure can be subdivided into two steps:

- the definition of general criteria, which must be met by the archiving procedure
- a concrete definition of the archiving procedure, on the basis of a decision model.

3.1. GENERAL CRITERIA FOR AN ARCHIVING PROCEDURE

In general, there are three types of criteria which a record keeping procedure must meet:

- legal: the legal framework in which a record keeping procedure operates, usually contains a number of limitations and/or obligations which must be observed. Especially, protection of the personal privacy, obligations with regard to the freedom of access to public records and the copyright law must be taken into account. Furthermore, specific laws or different regulations may be applicable for each type of record.
- archival science: the electronic records must conform to a number of archiving quality requirements such as a digital durability, the highest possible degree of autonomy and self-containment, the availability of required metadata, contextualisation, etc.
- implementation: the technological infrastructure, scalability, user-friendliness, co-operation and helpfulness of users, etc.



A preliminary study will provide criteria to which the record keeping procedure must comply. The possible archiving solutions are further delimited by each group of criteria, so that the record keeping procedure can be practically defined in the next phase.

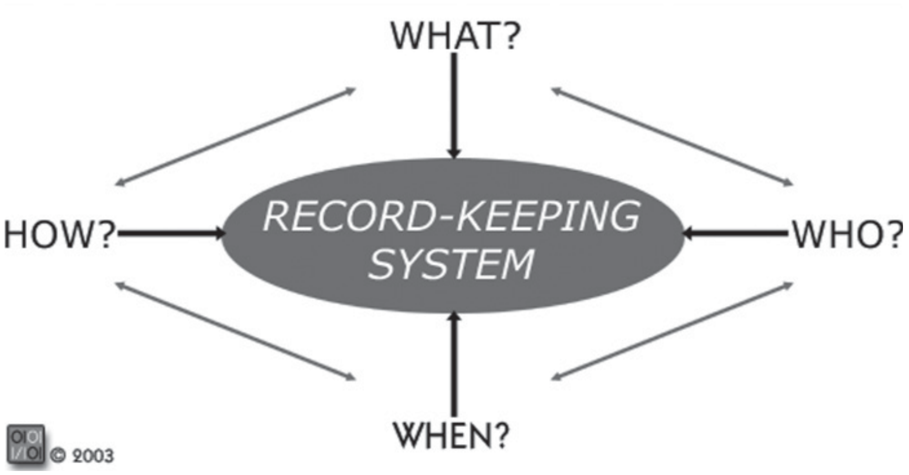
3.2. THE DAVID-DECISION MODEL

Once the general criteria have been defined, the building blocks of the actual record keeping procedure are defined in a following step. The DAVID-decision model can be used as a guideline in this regard. This decision model can be applied to the preservation of all types of electronic records.

Concrete choices are made on the basis of this decision model, which formulates an answer to four questions:

- WHAT is to be archived?
- WHO archives?
- HOW are record keeping actions put into practice?
- WHEN is a record keeping action carried out?

The basis for answering these four questions is the information system, in which the records are created, received or managed. It is typical for this decision model that an answer to one of the questions will/can determine the answer to some of the other questions. For instance, if the answer to the HOW-question is emulation, then this will also determine WHAT is to be archived.



3.2.1. WHAT is to be archived?

- Identification of records:
  - What are the records?
  - Which elements identify the documents that have a permanent archival value? What identifies the record: filename, unique ID number, etc?
  - Which components of the record are (permanently) preserved: content, structure, context, layout/look & feel, behaviour/functionalities?
    - => What are the essential and incidental properties of a electronic record?
    - => Which components give a document the status of a record?
- Will records be stored in their original file format, or are they only stored in their archiving file format?
- Are specific computer programs required for the reconstruction of the records (for instance emulation programs)?
- Which descriptive or technical metadata of the record will be archived?
- Which descriptive or technical metadata of the information system will be archived in which the record was created and/or managed?

3.2.2. WHO archives?

- Who creates the digital files?
- Who registers the descriptive metadata?
- Who registers the technical metadata?
- Who converts the documents to an archiving file format?
- Who deposits the records with the archival service?

Parameters:

  - Does the protection of personal privacy create limitations?
  - Is special hard- or software required?
  - Who has the required technical know-how?

3.2.3. HOW are record keeping actions put into practice?

- Which storage strategy will be used for digital objects :
  - Migration?
  - Emulation?
  - A combination of migration and emulation?
- In which archiving file format will documents be saved and preserved?
- How will the metadata be archived:
  - In a separate computer file?
  - Embedded in the same computer file that contains the record?
  - In a database?
- Which instruments/tools are used for the registration of the metadata and the conversion to archiving file formats?
- How will the old electronic records be archived? What tools are required in this regard?
- How are the records and their metadata deposited at the archival service?
- On what type of preservation media will the records and their metadata be stored?
- How will the authenticity and the integrity of the archived digital documents be guaranteed?
- How will it be guaranteed that records are not changed, after they have been stored.

3.2.4. WHEN is a record keeping action carried out?

- When will the record be stored? When is the record created? When is the document given the status and function of a record?
- Which steps in the archiving procedure are carried out at what time?
  - When does "capture" take place?
  - When are the records transferred to the archival service?

Parameters:

  - Capacity of the storage system
  - The retention period of the documents
  - The performance level of the computer system
  - Product support for the computer system
  - Replacement of the computer system, with which the documents were created or administered.

E. ARCHIVING PROCEDURES

1. BASIC PRINCIPLES

Concrete archiving procedures are developed and applied in implementation of the archiving policy. These archiving procedures translate the general policy into practice, and they are customised to the requirements of the organisation and its records.

Two archiving procedures have been detailed within the DAVID-project: one for office documents and another one for information systems. Both archiving procedures are based upon the general criteria for an archiving procedure and the DAVID-decision model. The electronic classification schema and its electronic files are the focus of attention in the procedure for office documents, while the procedure for information systems departs from the system itself. Tools and instruments were developed during the course of the DAVID-project for implementing both procedures. Despite their different starting points, both procedures share a number of similar procedural steps and instruments, such as quality control, registration and retrieval, application of archiving standards, etc.

The following basic principles were applied in developing these archiving procedures:

- application of the records continuum principle for the electronic records: the archiving procedure starts with the creation or receipt of digital documents, and it continues through to the ingest in the digital repository, their management and dissemination. This means that the archivist becomes involved with records management.
- integrating as many steps as possible from the "paper world", with which the user is acquainted (registration, filing, etc.).
- automation of as many actions as possible:
    - automation increases user-friendliness
    - automation enhances the correct application of the archiving procedure
- integrating the archiving procedure as much as possible into the existing IT infrastructure.

The implementation of this archiving procedure depends on a number of factors, not least the IT infrastructure in which the procedure is applied. In a first phase, the archiving procedure is applied in the existing IT environment as far as possible. After all, computer configurations cannot simply be replaced. In practice this will often mean that a number of (automated) records management functionalities will be built into existing configurations. To what extent this is possible depends, among other things, on the flexibility and the possibility for customisation of the installed operating systems and applications. The computer programs that are currently in use have their limitations in this area, but this isn't necessarily a disadvantage. It is even recommended that record management is at first organised within the existing IT environment before one proceeds to purchase and implement more advanced document and record management systems. In this way, the users can continue to work in a familiar software environment, and they will become acquainted with the required actions, such as the creation of electronic files and registration within a digital context. In the meantime, all of the involved parties will gain experience, and one will obtain a better insight into the specific demands that will be made on new software. This way one will be in a better position to define the functional requirements new software should meet from the point of view of records management, so that one will be able to apply the complete procedure in a second phase.

2. OFFICE DOCUMENTS

The DAVID-archiving procedure for office documents consists of six steps:

1. Developing a classification schema for electronic records
2. Creating and managing quality documents
3. Creating digital files
4. Appraisal and selection for long-term preservation
5. Migration to archiving file formats
6. Ingest into the digital repository and retrieval

The basic steps of the DAVID-archiving procedure for office documents can be applied within every IT environment. The implementation of an archiving procedure can proceed step by step. Not all of the steps of such a procedure must necessarily be operational at the start. Steps 1 to 3 are of primary importance. Once the procedure for creating a classification schema for electronic files is up and running, attention can be given to preparing the implementation of the remaining steps as well as to including the legacy records retro-actively in the archiving procedure or immediately into the digital repository. The first steps are primarily directed towards the creation of documents of a good quality, within a structured and controlled environment. Digital documents which are not created and managed in an organised and structured way are difficult to integrate retro-actively in a record keeping system, and it is very difficult to turn them into high-quality records. A pro-active procedure is therefore required from the moment of creation. If possible, these first steps should be linked as much as possible to an appraisal decision, so that the essential components of the records are determined in a structured way.

2.1. DEVELOPING A CLASSIFICATION SCHEMA FOR ELECTRONIC RECORDS

The development of a classification schema, in which electronic files and records are managed, is the first step in bringing digital documents under intellectual control.

An electronic classification schema structures the electronic files and organises the electronic records of the organisation. In this way, the archival context of the files and the individual items can be defined. By basing a classification schema or file plan on the business processes and the functions of the creator, a relationship is established between the files and the business processes in which they were created or received. After all, an archive contains process-related information and its goal is to document business processes. The file plan achieves this goal best, when it is a reflection of the operational processes that lie at the basis of records creation. If possible, it is also desirable to link the classification schema for paper and electronic records to each other. This is possible by applying the same structure, or by using common filing- or registration codes. In this way, the relationship between electronic and paper files can be indicated[16].

By classifying electronic files, the structure of the archive is made visible. Within the classification system the files are ordered in such a way that their (parent-child) relationship to one another is made clear. By assigning semantic folder names and/or adding descriptions, one can give additional meaning to the electronic records that are maintained within this structure. In this way, a logical and well-organised folder structure is developed, which communicates information about the context. This makes the files and their contents more easily accessible and usable by third parties, in stead of just by staff members responsible for the administration.

The file plan or the classification system not only forms the structure in which electronic records are archived, but it also delivers important metadata information about the records themselves. In combination with the names of higher-level folders, the folder name provides information about the archival context and indicates the location of the documents. This classification structure must not only be archived along with the documents; it is also recommended to foresee a way to reconstruct the classification system if necessary.

In short, a digital classification system is important from an archival point of view for a number of reasons:

- digital documents are created in a structured and controlled environment
- the bond between the file on the one hand, and the business processes on the other hand, is documented: since the documents are managed within their archival context, they can be understood and interpreted
- a link is created between electronic and paper files
- the file plan offers an overview of all digital documents which are at the disposal of the organisation: the folder structure strengthens the concept of digital information as a corporate memory or resource of the organisation
- the structure of the archive is made visible: records are more accessible
- creation of files: the link between electronic records is established; related electronic records can be managed as a group (e.g. appraisal and selection)
- a classification system makes appraisal and selection possible, so that an excessive preservation of files without archival value is avoided. Records should either be destroyed or archived in a timely manner.
- documents are accessible on the basis of consistent descriptions and the structure of the archive.

The organisation of records in a classification system is not only important from an archival point of view, but also offers a number of practical advantages:

- documents can be found more quickly and, as a consequence, will be re-used to a greater extent

- the same documents will no longer be stored in multiple copies at different locations: file servers will be unburdened and capacity problems will decrease
- greater clarity about the value and the importance of documents
- an easier application of version management.

Ideally, an electronic classification system is the result of collaboration between the creator, the IT staff and the archivist. It is advisable to take the time necessary to develop a joint folder structure, since this structure is the framework within which electronic records are created and managed. It must be possible for the end-user to find his way in this structure easily, as otherwise he/she may be discouraged from filing his records correctly. It is also recommended to foresee a procedure or agreements for the management and control of the classification system, from the moment that it is defined.

This first step is primarily directed towards the organisation of electronic files and records, and is applicable within each operating system. The currently used operating systems permit the creation of a hierarchical folder structure (Windows, Unix-Linux, Apple). The electronic classification system can be created and managed with the help of very simple file management applications (Windows Explorer, Nautilus File Manager, Mac Finder). These applications do, of course, have their limitations: no version management, limited access control, no possibility for the registration of self-defined metadata at file level, lack of functionalities for the indication of retention periods, limited search possibilities, etc. Within more advanced document management and record management systems, such functionalities are available[17].

Practical tips and recommendations for the creation of a classification system for electronic files are available on the DAVID-website:

- Digital ArchiVing. guIdeline & aDvice, no. 3: *Folder structure and file names for electronic records*.

2.2. CREATING AND MANAGING QUALITY DOCUMENTS

To enable a good record keeping system for electronic records, it is important to create documents of high quality from the beginning. This step is directed towards the creation and management of authentic, (re)usable and easily archivable electronic documents. Since the authenticity of the record is linked to its identity and its integrity[18], the necessary attention will be paid to these aspects in this step.

The quality of a digital document depends on:

1. the structure
2. the metadata
3. the file format
4. the reliability
5. the user.

The specific quality requirements of an electronic record depend on the function of these records within the business processes in which they are created and managed. Good records must remain related to the business processes, in which they were originally created or received (see sections 2.1 and 2.3).

The creation and the management of high-quality records will not only assure that the record keeping procedure proceeds more easily and more efficiently, it will also ensure that more incidental properties of electronic records are saved for the long-term.

2.2.1. The structure

The internal structure of a document is not only important because it is usually an essential component of an electronic record, but also because a successful migration is only possible when electronic documents are well-structured.

Together with the content, the structure of an electronic record is important for transmitting the purpose and the intention which is contained in the document over time. As a consequence, the structure of a record is in most cases an essential component. The structuring of a digital documents is closely associated with document modelling. This is one of the standard methods for communicating knowledge in an electronic way. The document model reflects the knowledge that originates after computer data are defined, identified and related. After all, computer data by themselves have no meaning; meaning is attained by defining and clarifying the relationships between the data. The internal structure also indicates how the different components of a document are linked to one another. The more the logical relations between the elements of a documents are indicated, the better a record will fulfil its function.

Success in the migration of a document depends substantially on the structure of the source document. Well-structured digital documents can be migrated more easily and with better results than unstructured documents. These latter documents are always more difficult to re-use outside of their original software environment. Well-structured documents will survive the ravages of time better, and it is easier to process them in an automated way.

As a consequence, it is important to structure digital documents internally in an explicit way. Documenting the structure of a document solely on the basis of its layout creates a substantial risk, since the layout is in many cases lost. It is better to use layout profiles and header styles, to which text-formatting can eventually be linked.

The granularity of the internal structure depends on the document model, and on the degree to which each component of the document must be (separately) re-usable or separately traceable.

2.2.2. The metadata

Digital documents can fully fulfil their function as a record in the future, when metadata about the document and its context are available. The quality of a record also depends on the quality of its metadata. Metadata fulfil a variety of functions, such as the identification of the record, supplying information about the archival context of digital documents, helping to guarantee long-term readability, assuring their reliability, etc.

Metadata, exactly like the electronic records themselves, must be permanent, stable and readable. Metadata are stored for at least the same period, as the digital documents to which they relate. Ideally, metadata of electronic records can be processed automatically. For metadata a number of quality requirements are applicable, namely they must be:

- fixed
- explicit
- structured
- digital
- readable in the long-term
- linked to a record.

With regard to the metadata of a record, and as a part of the DAVID-decision model, one has to ask oneself what metadata are registered by whom, at what level, and where they will be stored.

Which metadata are necessary depends in part on the type of electronic record and its function. For certain types of documents, metadata such as the author, version, title, date of creation, etc. are important, while these may be unimportant for other documents. The metadata of an e-mail, for instance, differ substantially from the metadata of an archived website.

Metadata can relate to a variety of different levels:

- the individual record: f. i. the title, author, version, date, a reference to the file folder or the subject matter, a description, keywords, reliability criteria, file name, software, etc.
- the file: f.i. the storage location, ID number, retention period, permanent archival value, related (paper) files, etc.
- the series: f.i. creator, function, handling, classification system, related documents, scope, begin-end date, the archiving history, etc.
- the archive: f.i. the creator, the mandate, function, handling, begin-end date, etc.

The metadata about electronic records can be stored in a variety of locations. Metadata:

- can be encapsulated in the electronic record (f.i. in the document profile/properties, in the fileheader)
- can be stored in a separate computer file
- can be included in a database.

In practice, a combination of these three possibilities is frequently applied and they largely depend on the way access is provided to the archived records. The advantage of encapsulation is that the metadata are indissoluble linked to the record, but such a decentralised storage has disadvantages regarding automated search procedures. The storage in a centralised database is therefore better, but this does require special care for a persistent link between record and its metadata. Regardless of the storage location, a long-term storage of metadata must also be taken into consideration. Encapsulated metadata, for instance, must be migrated along with the document to the target format (f.i. migration of the document profile of MS Word to XML, TIFF or PDF), and such a procedure may not lead to any readability problems. Databases, in which metadata are stored, are also subject to technological obsolescence.

Wherever possible, metadata are preferably registered in an automated way. After all, many metadata are already present in the computer system. In many cases this requires that the metadata are captured in a static and explicit way and are linked to the document or the file, to which they are related. Another possibility is to compose the metadata automatically. However, not all metadata can be registered automatically. Metadata about the archival context are a typical example of this. These metadata are best registered by those persons who know the contents and functions of the records best, which, in most practical instances, will usually be the administrative staff. If any action is required from the user in this regard, then it is recommended that a very user-friendly solution is provided. Otherwise, the risk that no metadata are assigned is very large.

Metadata are best registered when the document is created, or as quickly as possible after its receipt. Since the assignment of metadata is an incremental process, this must be taken into account.

2.2.3. The file format

The choice of the file format, in which digital information is stored, has direct consequences for the lifespan and the durability of electronic records. If possible it is highly recommended to store digital documents in a suitable archiving file format from the moment of their creation. This will help to avoid migration and the possible loss of incidental components.

In practice, though, this will not always be possible or desirable. For the purpose of functionality, reusability or user-friendliness, preference can be given decided to temporarily storing digital documents in a (non-exchangeable) manufacturer or application dependant format. In such cases, the migration path (target format, migration tool) must be known for this type of document at the moment of creation, so that, if necessary, special measures can still be taken during the creation process. Since in a desktop environment, the end-user can select the file format and a number of other settings himself, it is also highly important that clear guidelines and rules are communicated about this. If possible, the proper file format and profile should be preprogrammed, so errors can be avoided.

When a document is saved in a suitable archiving file format, one has to make sure that the applied file format profile is in conformity with the settings that are important from an archival point of view. Most archiving file formats can, after all, be composed in a variety of ways. The user is free to use a number of settings, but not all settings are equally suitable for long-term archiving. For instance, is not recommended to compose PDF documents with a PDF writer, or to apply JPEG compression when storing a TIFF document.

More information on this is available on the DAVID-website:

- F. BOUDREZ, *Standaarden voor digitale archiefdocumenten*, City Archives of Antwerp, Antwerp, 2002-2005.
- Digital ArchiVing. guIdeline & aDvice, no. 4: *Standards for file formats*.

2.2.4. The reliability

There's still no definte answer to the question how long-term reliability can be assured in a conclusive manner. In any case, the preservation of reliable records is only possible, when a procedure that assures such a reliability is applied from the moment of the creation or the receipt of such documents. After all, the reliability must be guaranteed for the entire life-cycle. Such a procedure must, in first instance, make sure that digital documents cannot be changed without authorisation and that changes are traceable. The emphasis lies on the protection of the integrity of the record. For this purpose, the creator can combine a variety of simple or somewhat more complex measures:

- access control and authorisation: only authorised users have access to files and records (for instance user IDs, passwords, biometrics, PKI)
- "read-only" access: after archiving or "capture", the electronic records are fixed and no longer changeable (protected folders and/or files, consultation only with a viewer software)
- version control: changes in documents can only be saved as a new version
- maintenance of an audit trail: registration of certain actions on documents (for instance, who changed what at what point in time?). Since it is practically impossible to log all actions, one has to define in advance which actions and what part of these actions will be registered. The log files that are utilised for system management will only be able to fulfil this function in rare cases, so the creation of separate audit trails may be necessary.
- hashing: storage of the hash codes that are calculated on the bits of the digital documents, so that subsequent verifications are possible
- time-stamping: registration of the date and the time of a transaction
- encryption: the transformation of the digital documents, so that they become unreadable for anyone who does not have the corresponding decryption key.

The reliability of electronic records is assured through a combination of procedures and technology. In this regard, one may not lose sight of the fact that technology is subject to ageing (obsolescence) and that procedures are required, to make sure that technologies can be replaced effectively. Such technologies are preferably also embedded in a general procedure, which guarantees reliability in the long-term. The (technological) components of these procedures must be replaceable, whenever the technology itself changes.

Since reliability is an important factor in an appraisal decision, and because of the necessity of demonstrating such a reliability, it is important that the creator documents his reliability procedures, and that these are made available to the archivist.

2.2.5. The user

And finally, the quality of digital documents is also determined through the users: the way in which digital documents are created, metadata are registered and the documents are organised.

The creation of high-quality digital documents, and in a next step the creation of files, depends on how familiar the are users with IT-processes and the level of care they take. As a consequence, making the users aware through training procedures is essential. The integration of basic skills for good document management in standard IT training courses for administrative staff members, is therefore recommended. Since the creation of good digital documents imposes some limitations on the user in a number of different cases, it is also important to provide motivations for those limitations.

2.2.6. Implementation and examples

The creation of quality digital documents depends strongly on the way users compose documents and save them. This process can be steered in the right direction by providing the necessary training and through the creation of standard documents or the use of templates. Templates can be used to fix the structure of a document in advance, and perhaps also to anticipate on future migrations of the documents, for instance by registering dynamic data in a static and explicit way. Furthermore, templates also include the possibility of assigning metadata in an automated and user-friendly way.

With templates, certain actions can be carried out in a completely automated or user-friendly way. Office applications, such as MS Office and OpenOffice, permit the use of macros and scripts with templates.

Two examples of such templates are available on the DAVID-website:

- an e-mail template with a script:
    - automatic registration of metadata: e-mail address of the sender, date and time-stamp of the transmission and receipt, file names of the attachments are captured in an automated and structured way
    - user-friendly assignment of the reference code and the target folder by the sender or receiver
    - export functionality: storage in a predefined file format, separation of the e-mailmessage and attachments, replacement of impermissible characters in file names
- word template with macro: mandatory adding of pre-programmed and customised metadata in an automated and user-friendly way, which is achieved at document level by a user through the opening and closing of a text processing document.

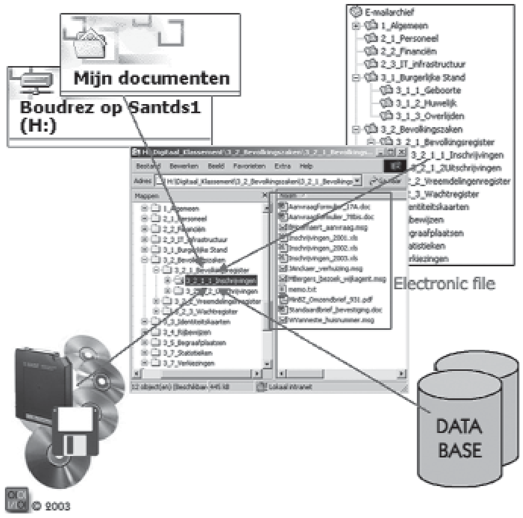
Tips and recommendations for good digital documents:

- give office documents a clear identifier (f.i. filename, referencecode, etc.)
- define the internal structure of documents in an explicit way; define the structure with the help of (header-)styles, instead of only using text-formatting
- make sure that the content of dynamic fields (for instance an automated date field) is fixed as soon as the document has been completed
- make agreements about the re-use of documents, and for the creation of new versions of an existing document, after the original version has been captured in a definitive way.

2.3. CREATING DIGITAL FILES

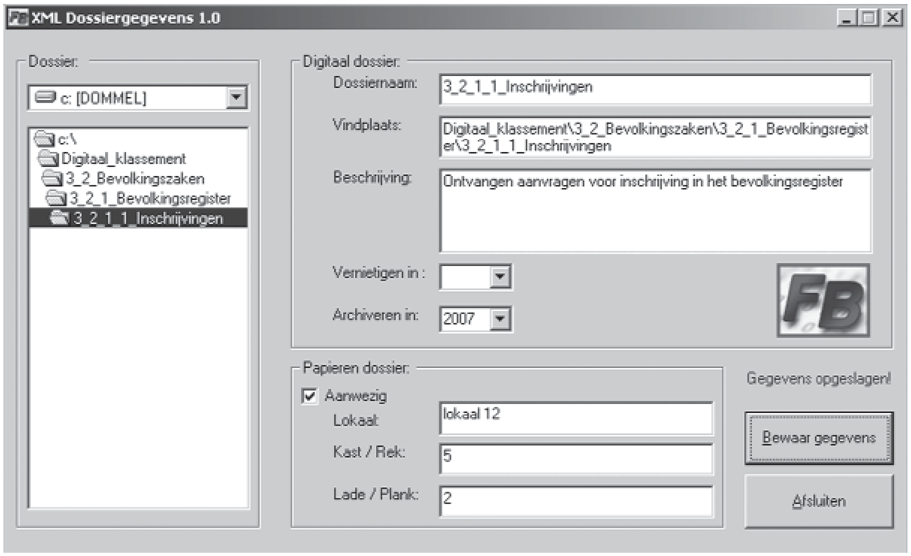
Digital files are created and managed in a digital classification system. All digital documents which are related to a task, a file or a subject, are stored in the same folder. In this way, a relationship between related documents is defined.

The creation of electronic files offers the advantage that the possible finding places of electronic records within an organisation are reduced to one central location. Instead of spreading documents over local hard disks, file servers, e-mail systems, database systems, external storage media, etc., the electronic records are collected in a centrally managed classification system. In this way one obtains a quick overview of all available information within the organisation and of all records related to a particular event or subject, regardless of the type of document or application in which these documents were created: text documents, spreadsheets, e-mail messages, presentations, etc. This is the way to prevent the creation of several information islands within an organisation. Information islands sometimes come into existence, because specific applications are used for the management of a certain series of records (decisions, correspondence, e-mail messages, etc.). These applications are not suitable for storing large quantities of records in the (medium) long term. It is better to add the records of such a series to an electronic file, instead of managing them within these applications.



The structured classification of electronic records by file or subject folders, makes it possible for the administrative staff or archivist to process those digital documents as a group. Appraisal and selection can, for instance, be carried out at a file or subject level. This has, however, consequences, since dropping a document in a certain folder is connected to a decision with regard to its preservation or destruction. Close supervision is recommended in this regard, but is not always easy to achieve.

An essential aspect of the creation of electronic files is the registration of metadata about these files. Important information about electronic files are amongst others: their position within a certain work process, a description, their relation with and the location of a related paper file, the documents in the file, and the retention period. These metadata are common to all documents within the file, and they must be linked to the electronic file in one way or another. That is how a file profile is developed. Most commonly used operating systems of today do not offer the possibility of registering customised metadata at folder level. However, this is possible with WebDAV, or with more advanced document management systems. An inbetween solution is the ad hoc application, which has been designed by DAVID. This application offers the user an interface to add metadata about an eletronic file, and these file attributes are saved as an XML document in the folder to which the metadata are related[19].



c: [DOMMEL]

c:\
Digitaal_klassement
3_2_Bevolkingszaken
3_2_1_Bevolkingsregister
3_2_1_1_Inschrijvingen

Dossiernaam: 3_2_1_1_Inschrijvingen

Vindplaats: Digitaal_klassement\3_2_Bevolkingszaken\3_2_1_Bevolkingsregister\3_2_1_1_Inschrijvingen

Beschrijving: Ontvangen aanvragen voor inschrijving in het bevolkingsregister

Vernietigen in :

Archiveren in: 2007

☑ Aanwezig

Lokaal: lokaal 12

Kast / Rek: 5

Lade / Plank: 2

The electronic files are the building blocks of the classification system. Since the following steps in the archiving procedure take this classification system as their starting point, one can consider the inclusion of a document in a certain file folder as the formal transaction with which the document effectively becomes a record for the organisation. Digital documents, which are not a part of this classification system, effectively escape the archiving procedure and will not be included in the digital repository. One could say that adding a document to a classification system "classifies" the recordstatus of a document.

The classification structure itself and the location of electronic records within this structure are important metadata information. The file folder structure reflects the context in which the documents are created or managed and indicates the relationship between the documents and within a business process. As a consequence, the folder structure must be archived and should be documented extensively. A loss of the folder structure would, after all, mean a loss of the archival context. It is one of the essential components of a record. A possible solution for this problem is the creation of XML file lists. A hierarchical overview of the folders is created in such a file list, including a mention of the documents that are stored in those folders[20].

2.4. APPRAISAL AND SELECTION FOR LONG-TERM PRESERVATION

The issues regarding appraisal and selection are situated at two different levels within the digital world: the file and the records. At file level, the question regarding selection focuses above all on which files are preserved and which are destroyed. At record level, based on appraisal a decision is made as to which components are essential and which are incidental. In case of paper documents, this last question does not pose itself because the entire paper record is preserved.

The records schedules for paper files are equally valid for electronic files. No other retention periods apply for electronic files. Brought into practice this means that at a given point in time, those files, which are considered for long-term archiving, are selected and removed from the active classification structure. Such a selection can be carried out on the bases of a manual and/or automatic selection procedure. The latter method, however, requires that the retention period is indicated and processable in one way or another. One possibility is, for instance, to include the retention period and the disposition in the metadata of the file.

For appraisal and selection, it is not an unnecessary luxury to register metadata at file level. These metadata provide information about the context and the value which the creator assigns to the files in the electronic classification system. The fact that administrative staff members have assigned storage periods does not replace the need for retention schedules. Quite to the contrary, the assignment of a retention period is based on the records schedules or on archival management plans. These are developed by the records creator and the archivist, and they immediately indicate what importance the creator gives to certain files.

At document level, the problem concerning appraisal and selection is actually continuously present in the archiving procedure. It must actually be known from the moment a document is created, which components of the document are essential and must therefore be archived, so eventually the necessary measures can be taken. The same question arises again before deciding on a migration path to a suitable archiving file format, and it must be answered every time the record is migrated once more in the future. The result of appraisal will, after all, contribute to making a decision about the file format that is used as an archiving file format. The essential properties have to be included in the archiving file format. The archiving file format must therefore support these properties and permit their maintenance in the future. Incidental properties may be lost or changed during migration.

2.5. MIGRATION TO ARCHIVING FILE FORMATS

After selection and before digital documents are included in a digital archive, they must, if necessary, be migrated into a suitable archiving file format. This offers two advantages:

- first of all, only electronic records with permanent archival value are migrated, which saves costs and time
- and secondly, the migration can occur under the responsibility of the creator, who can declare migrated documents as authentic.

Those electronic records, which are stored in an archiving file format from the moment that they are created, need not be migrated. It is recommended to check whether the correct settings from an archival point of view were used. If necessary, compression, encryption, passwords, etc. must be removed,

Migration to a suitable archiving file format is preferably performed with reliable migration tools, which are capable of migrating large quantities of digital documents automatically. The quality of the migrated documents depends strongly on the computer program that is used for the migrations. Special requirements are therefore applicable to migration tools:

- a 100% correct application of the file format standard or specification
- the possibility of configuring which profile of the archiving file format to apply
- reliable and error-free migration: extensive testing!
- error-detecting and reporting: registration of which documents were not successfully migrated, so that these can subsequently be migrated manually
- quality control of the migrated documents.

Both commercial or open source tools can be used for the migration, existing computer applications can be customised, or custom software can be developed. Adapting existing applications oneself, or programming custom software, offers the advantage that one determines the functional requirements for the migration tool oneself. Also, one can better understand the operations that are carried out behind the scenes. Availability of and control over the source code of the migration tool, as well as a full documentation thereof, is almost indispensable on order to be capable of verifying and demonstrating the reliability of the migration operation.

More information on this is available on the DAVID-website:

- Digital ArchiVing. guIdeline & aDvice, no. 10: *Migration to archiving file formats*.

Tips and recommendations:

- take old hard- and software out of operation only after you have carried out a quality control on the migrated documents. Remove certain hard- and software only after you have made sure that all data with archival value, which has been created with that hard- and software, can still be consulted with the migrated versions.
- check and document the source code of the conversion applications. Specify in the contract that the source code of custom software is documented by the programmer and is transferred along with the installation files of the application.

2.6. INGEST INTO THE DIGITAL REPOSITORY AND RETRIEVAL

2.6.1. Verification and registration

On receipt in the archival service, the transferred documents must be verified and registered.

The verification of the transferred electronic records includes:

- the completeness of the transfer: does the storage media contain all records (for instance, a check on the basis of an XML file list, which has been used as a transfer list)
- quality of the electronic records: integrity of the bitstreams (MD5-check on the bitstreams); are they stored in a suitable archiving file format (identification of the file formats); has the correct archiving profile been applied (validation of the file formats); have clear file names and the correct filename extensions been used; have the files been provided with metadata?
- the presence of instruments for record retrieval
- the quality of the transfer storage media, whenever these also serve as the long-term storage media
- computer viruses.

Whenever, during such a verification, problems are detected or the predefined quality requirements are not observed, the creator must be contacted and asked to resolve these problems.

After a positive evaluation of the quality, the creator is given permission to delete the documents and the new acquisitions are registered. Then an inventory of the records is prepared and their metadata are completed. In this regard, attention must be given to the presence of a unique ID number for each of the electronic records. During registration, the metadata at file and/or document level can also be indexed and included in a database, so that centralised search queries are possible.

2.6.2. Searching for archived files and records

The user can be given access to the archived electronic records on a variety of different levels:

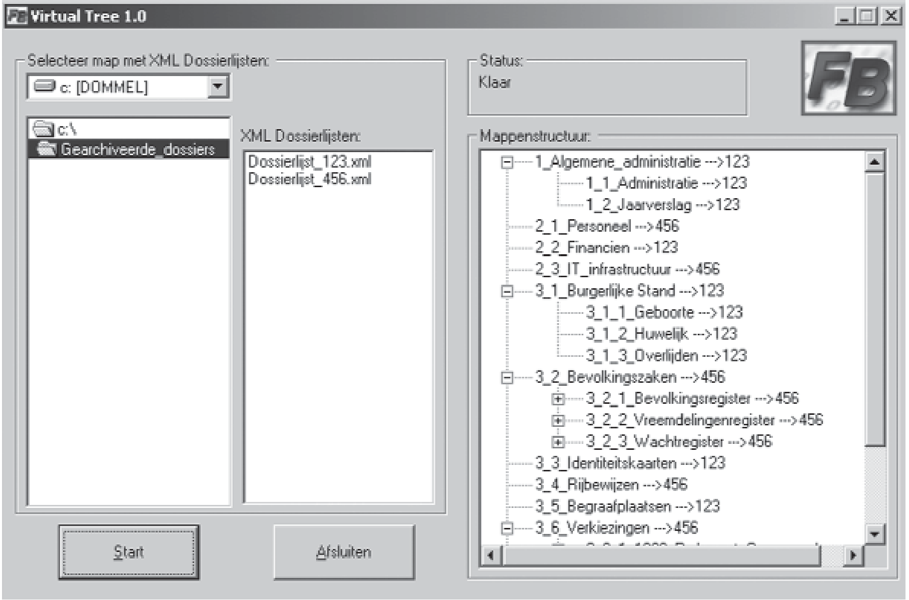
1. series
2. file
3. document.

Giving access only at a series (type) level, such as for instance "personnel files", is too general to allow archived files and records to be retrieved efficiently. Searching at file and record level are more interesting, as this allows for more targeted searches. We will discuss how records can be searched for and located at both levels below. Two methods are provided for this:

1. via storage of metadata in a database
2. via XML file lists.

The level and the way in which digital files and records are queried, depends primarily on the availability and the storage location of their metadata. Efficiently searching through all metadata is only possible, when these are stored in a central database. In order to give access at file level, this means that the metadata of all digital files must be known, and can be processed. If these metadata have been stored in a digital, explicit and structured way, they can be included in the database automatically.

Giving access at record level depends also on the availability of metadata (for instance the file name, author, a subject description, keywords, etc.). A more detailed search procedure on words that are included in the documents is an option. This means, however, that the records must be indexed, and that the full-text index has been added to the database which includes the metadata.



c: [DOMMEL]

c:\
Gearchiveerde_dossiers

Dossierlijst_123.xml
Dossierlijst_456.xml

Klaar

```
⊟ 1_Algemene_administratie --->123
      1_1_Administratie --->123
      1_2_Jaarverslag --->123
  2_1_Personeel --->456
  2_2_Financien --->123
  2_3_IT_infrastructuur --->456
⊟ 3_1_Burgerlijke Stand --->123
      3_1_1_Geboorte --->123
      3_1_2_Huwelijk --->123
      3_1_3_Overlijden --->123
⊟ 3_2_Bevolkingszaken --->456
    ⊞ 3_2_1_Bevolkingsregister --->456
    ⊞ 3_2_2_Vreemdelingenregister --->456
    ⊞ 3_2_3_Wachtregister --->456
  3_3_Identiteitskaarten --->123
  3_4_Rijbewijzen --->456
  3_5_Begraafplaatsen --->123
⊟ 3_6_Verkiezingen --->456
```

Searching for files and records is also possible on the basis of XML file lists, which were created as documentation of the electronic classification system, and which were also used as a transfer list (see item 2.3 and 2.6.1). This method does not make use of a database, in which all the files and/or document metadata have been included, instead it offers the user a searching mechanism that is based on the data that is included in the XML file lists. The function of XML file lists is once more expanded in this way.

On the basis of the XML file lists, the electronic classification structure of a creator can be reconstructed, so that search operations remain possible on the basis of the classification system, even if the archived files have been removed from the active classification structure and have been distributed on several storage media. For the reconstruction of the classification structure and its contents, the various XML file lists of one particular creator are merged. For such an operation the XSLT-technology can be used. A desktop application can be developed for this purpose or one could offer this functionality as a webservice in which a webpage with the merge or search result are sent to the user.

Searching records is a two step process in this case. The user first searches for the relevant files, by browsing through the business processes, tasks and activities of the creactor. Subsequently, the desired document is searched for within the located folder. Such a search procedure proceeds primarily on the basis of the file name of the document. Since the file names of the records have been included in the XML file lists, they can, if required, be displayed under the folder names in the interface with the search results. Also the file type can be a guideline during a search procedure. Since the search procedure is now already refined to searching within a certain folder, an "on-the-fly" query of the content of the documents can proceed more quickly and in a more targeted way. However, in the case of large quantities of documents, this is not a recommended or efficient way of working, since the documents must be searched one by one.

The search path, when accessing the archives on the basis of an XML file list, remains largely limited to the structure of the archive which is based on the business processes, tasks and activities of the records creator. This can be sufficient for those users who are acquainted with the actions of the creator, such as administrative staff members and civil servants. This is less suitable for external users of the archives. The archived files and records must be made accessible in a more explicit way for them, and the records must be placed within a context, so that they can follow other search paths. XML topic maps could be a solution for this need. On the basis of a topic map, an external user can retrieve archived files and records, based on his own associations and search paths. The XML file lists can be used as building blocks for an XML topic map.

More information on this is available on the DAVID-website:

- F. BOUDREZ, H. DEKEYSER and S. VAN DEN EYNDE, *Archiving e-mail*, City Archives of Antwerp – ICRI Leuven, Antwerp-Leuven, 2003. (DAVID-rapport no. 4).

- F. BOUDREZ, *E-mails: hoe bewaren en goed archiveren?*, Technical report of the City Archives of Antwerp, Antwerp, 2003.
- F. BOUDREZ, *Hoe archiveer je digitale kantoordocumenten*, in: Lokaal, no. 7, april 2003, p.17- 19.
- F. BOUDREZ, *<XML/> and electronic recordkeeping*, City Archives of Antwerp, Antwerp, 2002.
- F. BOUDREZ, *XML Topic Maps voor digitale archivering*, City Archives of Antwerp, Antwerp, 2002.
- DAVID-cases:
- e-mail.

3. INFORMATION SYSTEMS

3.1. CHARACTERISTICS

Besides digital office documents, organisations maintain large-scale information systems with which digital information and documents are created, managed and distributed. Examples of such information systems are websites, geographical information systems, applications for the management of all kinds of registers, delivering permits, postal registration, follow-up of file handling, etc.

These information systems have a number of typical characteristics, which make a separate archiving procedure necessary for each of them. These characteristics include the following:

- that the information systems are usually controlled by databases. That the data and/or the documents are stored in database systems, which in turn are part of an integrated whole of interactive applications.
- that the data which is created and managed in these systems does not always have a fixed documentary form. This is a consequence of the use of new technologies, and the fact that data, not documents, serve as their basis.
- that the documents are usually re-composed at the moment that they are requested, and that they are not statically stored as a document as such. That the content of the documents depends on the information which is available at the moment of the interaction with the user.
- the data/documents are integrally managed centrally on mainframes and servers, and they cannot be structured by creating files.

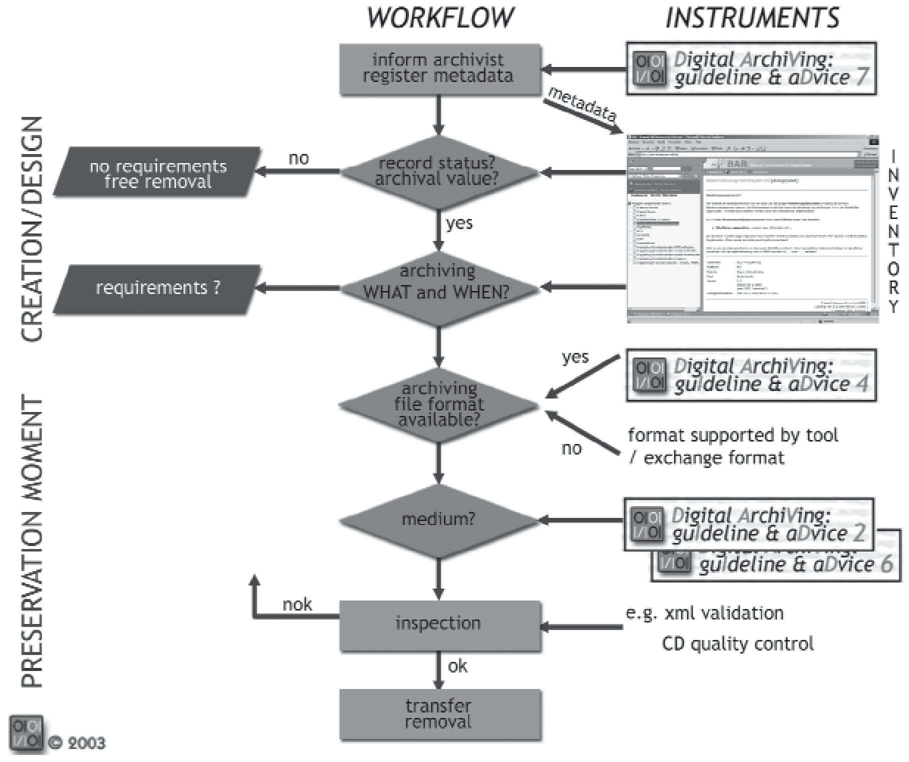
A consequence of these characteristics is that "capture" (identification, storage and registration) of the records is an essential part of the archiving procedure for information systems. The records are identified in these data-centric information systems on the basis of appraisal. The dynamic and interactive character of these information systems, and the largely indeterminate documentary form of many of the documents in these systems, does not make this self-evident.

3.2. THE INFORMATION SYSTEM AS STARTING POINT

The starting point for an archiving procedure is the information system, in which the documents are created and maintained. There is such a large variety and complexity in information systems that each should be analysed to find out its specific characteristics. Particulary the architecture, the functionalities, the dependencies, the workflow, the interactions, etc. differ from system to system, so that the archiving procedure must depart from the information system itself, so as to be able to determine WHAT needs to be archived HOW and WHEN. Since the information systems are usually managed on a completely centralised basis, the answer to the WHO question is in most cases the system administrator, but exceptions are possible.

3.3. WORKFLOW AND INSTRUMENTS

Just as with office documents, the archiving procedure for information systems starts with the creation up to the ingest into the digital repository and giving access. The first steps in the archiving procedure are taken at a very early stage. The archiving procedure starts with the design and the development of the information system, in which the documents are created and managed, i.e. before the actual creation of the documents themselves.


WORKFLOW
INSTRUMENTS
CREATION/DESIGN
PRESERVATION MOMENT
inform archivist register metadata
Digital ArchiVing: guideline & aDvice 7
metadata
INVENTORY
record status? archival value?
no
no requirements free removal
yes
archiving WHAT and WHEN?
requirements ?
archiving file format available?
yes
Digital ArchiVing: guideline & aDvice 4
no
format supported by tool / exchange format
medium?
Digital ArchiVing: guideline & aDvice 2
guideline & aDvice 6
inspection
nok
e.g. xml validation
CD quality control
ok
transfer removal
© 2003

The procedure starts with informing the archivist and the registration of metadata about the information system.

The creator informs the archivist about the development of the new information system, the adaptations to an existing information system or the dismantling of an outdated information system. It is best to include this notification obligation within the organisation as a formal step in the general IT procedures. Preferably, such a notification should be done as early as possible, so that the archivist has the required time for an analysis and anticipative measures, and does not lag behind the facts. The aim of this step is informing the archivist so he knows for what type of information system an archiving solution is required, so that he will be involved in the development, the adaptation or the dismantling of the corresponding information system.

Since the archivist requires information about the information system for planning his following steps in the archiving procedure, it is important that documentation about the information system is provided for registration and maintenance as early as possible, and in a structured and organised way. Metadata about information systems are, however, not systematically maintained in most administrations or IT departments. As a consequence, archivists only dispose of the information system itself at the moment of archiving, in the best of cases including some verbally provided information about the system. It speaks for itself that this is an insufficient basis for important decisions, such as the identification of records, appraisal and the development of an archiving strategy.

The metadata about information systems are registered and maintained in a new archiving instrument: an information systems inventory. From the day of its creation, metadata about the electronic information system are maintained in this inventory by the creator, the system administrator(s) and the archivist. The basic data model for this management inventory are the data fields that are required from an archival point of view. These refer to the creation context, the technical context and the management context. Such an information systems inventory can, however, also serve other goals, such as a helpdesk function or the management of the IT infrastructure. In this way, this inventory offers an added value for the entire organisation, whereby the creator and the archivist are not the only interested parties for keeping the inventory up-to-date. An information systems inventory can take on a variety of forms. It can evolve from a simple text file into a substantially more advanced database application. The information systems inventory of the City of Antwerp, for instance, is a relational database with a web based interface, including a dynamic data model.

Based on the information in the information systems inventory, possibly supplemented through additional documentation, the archivist identifies the records within the system, and he examines whether documents with archival value are being created. Before new systems are implemented, the archivist can examine demo versions or technical data sheets / descriptions of the information system. Since no documents have yet been created in this instance, it is highly important to link the appraisal to the business processes in which documents are created, as well as to the function that they fulfil in these processes. In the case of adaptations or dismantling of existing systems, the information system itself is an important source.

With regard to databases, the archivist must examine whether:

- the database itself is a record
- the database is an aggregation of records
- a particular output of the database are the records.

During the process of identifying the records, the archivist must also define the boundaries of the record. Many information systems are, after all, linked to one another and extract information from external sources. On the basis of the identification of the records and appraisal, the archivist determines whether the external information is archived as a part of the information system or separately.

If no records are created within the information system, then it speaks for itself that no archiving procedure is developed, and also that from an archival point of view no special requirements are defined for the information system.

archiving WHAT and WHEN?

If records are created and managed within the information system, then the archivist will answer the WHAT and WHEN questions of the DAVID-decision model. It is important to link these questions immediately to a retention period for the records, and also to the requirement for archiving stable and fixed (non-dynamic) documents.

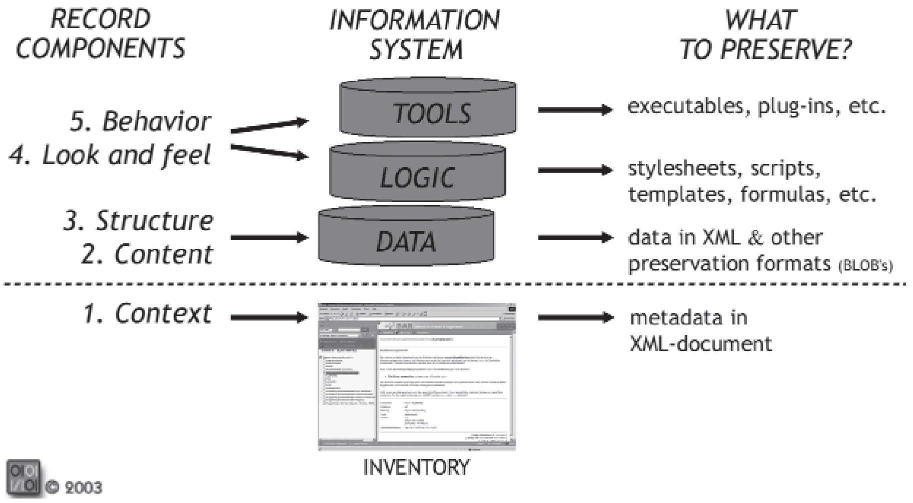
Records with a limited retention period, or those where the lifespan is limited to that of the information system itself, can probably be preserved within the active information system, whereas a long-term solution must be provided outside of the information system for those documents with a long-term preservation requirement.

- in the first case, the archivist will see to it that the records are maintained and can be consulted in the information system itself
- and in the second case, the archivist will see to it that the records are captured as conceptual objects, so an interpretation is possible in the future without recourse to the original information system.

On the basis of an identification of records, appraisal and the retention periods, the archivist will examine which components of the information system must be archived for the long-term. The choice of the components of an information system, which are or are not archived, is not only dependent on the classical archiving criteria. Such a choice depends also on the technical requirements for faithfully reconstructing the records in the future.

In order to answer the WHAT question it may be usefull to view the information system as a composition of three interactive layers:

- the data: the complete database, a part of the database (datasets) or a certain output from the database
- the logical components: those elements that process input and generate output
- the tools: the instruments or applications for input, output and display.



These three layers can be linked to the five components of the record. An identification of the essential and the incidental components of the record will determine, which layers or which parts of that information system are archived. In this way a differentiation is, for instance, made in the data layer, between computer data and records, whenever the database is not the complete document itself. The records are collected by a query, which is created on the basis of appraisal. The result of this query will subsequently be exported from the database system and archived. When, by contrast, the database itself is the record, then substantial attention must be paid to the structure. The parent-child relationship is important for hierarchical databases, whereas the relationship between the tables and the structure of the records must be archived together with relational databases.

The context of a record is somewhat of an exception in this case, since the context is usually not an integral part of the information system itself. Since the context and the metadata of the information system are documented in the information systems inventory, both can be distilled from this inventory.

For those records, which are taken into consideration for long-term archiving, it is recommended to define WHEN they will be removed from the information system. An answer to the WHEN question can depend on a number of different factors:

- limitations of the storage system
- the performance level of the computer system
- support by suppliers
- replacement or upgrade through a new information system.

Regardless of the retention period, and on the basis of the WHAT and WHEN questions, this step examines whether there are special requirements that apply to the information system, with regard to the creation, maintenance and an efficient archiving of good electronic records. These requirements can refer to such items as:

- the encoding of data: application of standards, storage of documentation
- the file format in which the documents are stored and the quality requirements
- the registration of metadata
- the archiving of changes, or the creation of a version history
- the registration of documentation
- the integration of reliability guarantees and measures
- the provision of an archiving module, so that documents can be archived in a simple and automated way.

The transient and interactive character of information systems is frequently in conflict with the stable characteristics that are required of records. The data in databases are continuously augmented or changed, while records, per definition, take a fixed documentary form with a permanent content. Because of the necessity for reconstructing data, it is frequently recommended to maintain a history of the data and their changes. Such a history can be maintained either within the database itself, or outside of the database in the form of a log file. If one opts for the latter solution, then it is best not to use the log files that are automatically created by database management systems. The primary goal of such log files is general database management and recovery, and, as a consequence, they are not so very suitable for archiving purposes. The standard log files also contain much information that is not important for archiving, meaning that these files become very large and are not easily deciphered. It is better to create a separate log file for archiving, and to determine in advance the actions that need to be registered, as well as what parts of these actions are to be logged in the log file. In this way one can limit the size of the log files and assure that they are more usable for archival purposes. Both questions are best answered from an identification and evaluation of the records. It is self-understood that one will take this into consideration, starting from the time that a database is created. By the way, this also applies to the audit trails that are created and kept.

At the latest, at the moment of archiving, the records are converted to an archiving file format. A suitable archiving file format will be available for a number of different types of digital documents. The archiving file formats that will be utilized by an archival service are preferably defined in a formal way in advance. With this, the format profile and its ideal archiving settings are defined for every format. In the absence of a suitable archiving file format, the records are stored in an exchange format. If no other solution is available, then storage in the application-dependant format is a (temporary) solution.

Which archiving file format is actually used, depends primarily on WHAT is being archived. Since only the content (or better the documents) is archived, but not the database system as such, the same archiving file formats that are used for office documents can be utilized. In practice this can mean that the data from a GIS application is stored as a GML document, or that charts and maps are archived as GeoTIFF or SVG files. XML, together with ASCII or Unicode, is the recommended archiving file format for purely textual databases. Binary objects that are stored in a database, or the generated output of such data, are best converted to the archiving file format that is most closely linked to their type.

In most cases, it is advisable to define the archiving file format at the time that the archiving procedure is developed. This is not always possible in practice, in which case is better to wait and see what options are available at the time that one proceeds to archive. Information technology and standardization are, after all, continuously developing.

The next part of the question is the HOW aspect of the decision model, concerning the preservation medium that is used for transmission and/or long-term storage. The archival service determines which media are used for transferring data. In principle, every type of storage medium can be taken into consideration, which can be read by the archiving service. A transfer of data files via networks is possible, however it is not self-evident when large quantities of computer files must be transmitted. The archival service transfers these files to a suitable long-term storage medium.

Matters become somewhat more complex, when the archival service also wants to use the transfer medium as the long-term storage medium. Strict quality requirements, for writing data to and manipulating it on these storage media, are applicable in this case.

inspection

In the next steps of the procedure, the transmitted documents are checked. Precisely as in the archiving of office documents, both the electronic records and the media on which they are stored are checked for completeness, quality and the availability of metadata. Examples are validation of XML documents, random sample tests of binary formats, quality control of CD-r's, etc.

When the transferred data do not successfully pass the quality checks, then any errors or problems must first be corrected and certain actions may have to be repeated. It is consequently very important that the information and/or documents have not yet been deleted from the information system, and removal is postponed until after a successful check of the quality of the transmitted data.

transfer
removal

The records are registered and made accessible, when the transmission meets all quality requirements. Only then does the creator get the permission from the archival service to remove the records, or to dismantle the entire information system.

More information on this is available on the DAVID-website:

- F. BOUDREZ, *The digital recordkeeping system: inventory, information layers and a decision-making model as a point of departure*, City Archives of Antwerp, Antwerp, 2001 (DAVID report no. 4).
- F. BOUDREZ, *Preserving electronic records from database-driven information*

systems, City Archives of Antwerp, Antwerp, 2003.
- F. BOUDREZ, *Preservation of electronic records from database-driven information systems*, ErpaWorkshop: *Long-term preservation of databases*, Bern, 9 April 2003.
- F. BOUDREZ, S. VAN DEN EYNDE, *Archiving websites*, City Archives of Antwerp – ICRI Leuven, Antwerpen-Leuven, 2002 (DAVID-rapport no. 5).
- DAVID-cases:
    - electoral register
    - population register
    - preservation of websites.

F. CONCLUSION

Digital archiving offers several challenges, but isn't a long way off. However, one must be aware that there are no solutions out of the box for electronic record keeping. Digital archiving is all about developing and implementing an efficient electronic record keeping system. Procedures and technology are the core of such a system. When developing a record keeping system, one has to keep in mind that procedures and technology have to be implemented in the right perspective.

Archival science must provide the leading guidance in tackling the problems involved with the long-term preservation of electronic records. Especially the identification of the records and their appraisal are the keystones for every record keeping procedure. Defining exactly what has to be preserved for the long-term, allows a reduction of the problems and makes digital archiving a feasible mission for every organisation. Archival science must also be the main basis for the long-term digital preservation strategy for electronic records. One can not merely rely on technological approaches or solutions alone.

After all, a potential risk is that a record keeping system is too much dictated by one technological solution. The implementation of a record keeping procedure is far more than just installing new software with record keeping functionalities. The record keeping procedure, preferably based on a formal policy, needs to be the framework and is the only thing which will survive technological obsolescence. Technological solutions have to be embedded within this procedure and must be replacable whenever there's need to. The DAVID-decision model can be used for developing such a record keeping procedure. The practical implementation of the record keeping procedure will be different for every organisation.

However, this does not mean that technological solutions aren't an important part of every record keeping procedure. As we want to preserve the digital nature of electronic records, we will always have to rely on some kind of technological solution for giving access to the preserved records. At the moment, the technological solutions to solve a wide range of obstacles are available today and are ready to implement. When choosing tools and instruments, one has to make sure that these are tuned with the organisation's overall procedure and more particular with its digital preservation strategy for the electronic records and their metadata.

In any case, it's recommendable to start the record keeping procedure before the actual electronic records are created. This is the only way to apply an effective record keeping system. By doing so, one can also save on the investment of time and resources. Retro-active archiving initiatives will never have the same result. This has a lot of consequences, not only for the archivist but also for the IT-users and the IT-developers.

One of the consequences for the archivist is that he moves forward in the lifecycle of electronic records. This is certainly the case when there's no tradition of records managers in the agencies of the creator, like in Flanders or even in Belgium.

REFERENCES PART 1

[1] Law of 24 June 1955 (*Moniteur belge*, 12 August 1955).

[2] Article 1921ff. of the Belgian Civil Code.

[3] BALLON, L., "Het Bewijs en de Moderne Technieken", DA/OR, 1990/4, 65.

[4] Article 1315 and following of the Civil Code.

[5] Contrary to the rules of evidence in tax matters and in criminal cases where, in principle, every type of evidence is admissible and the court judges its credibility.

[6] The concept "evidential value" relates to the faith that the court places in evidence. It is only when the court has assigned evidential value to an piece of evidence that one can speak of proof. In principle, it is the court that judges the evidential value of the evidence submitted to it. For some pieces of evidence, such as the signed document, the law determines the evidential value.

[7] The law did not define the concept signature before the electronic signature was introduced. This definition was developed in jurisprudence and in doctrine.

[8] The civil rules of evidence are not considered a part of the *ordre public* which the courts must uphold on their own initiative. Ludo Cornelis and Lucien Simont, "Bewijsrecht en Technische Evolutie: Enkele Overwegingen", in Paul De Vroede (ed.), *Technologie en Recht*, Antwerp, Kluwer, 1987, 152-153.

[9] The problem resides in the value of electronic documents as evidence. There is no difficulty now (nor was there in the past) with the validity of agreements reached electronically. There are no special formal requirements, such as drafting a signed document; that must be satisfied for an agreement to be valid. A consensus among the parties is sufficient.

[10] Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 on a Community Framework for Electronic Signatures, *Official Journal of the European Communities* 19 January 2000.

[11] The law of 20 October 2000 introducing the use of telecommunication means and of the electronic signature in proceedings in and out of court (*Moniteur belge* 20 December 2000).

[12] The law of 9 July 2001 on the establishment of certain rules relating to the legal framework for electronic signatures and certification services (*Moniteur belge* 29 September 2001).

[13] See annex 1.

[14] A digital signature is code that is illegible for humans; it could look something like this: Xh7%^[!Fsa3g3°hHY.

[15] The law of 20 October 2000 adds a section to article 1322 of the Belgian Code of Civil Law which states, "A set of electronic data, which can be attributed to a particular person and which can demonstrate the preservation of the integrity of the document, can satisfy the signature requirement for the application of this article."

[16] Art. 4 §5 of the Certification Services Provider Act.

[17] Art. 4 §4 of the Certification Services Provider Act.

[18] Annex I to the Certification Services Provider Act.

[19] Art. 17§1 of the Certification Services Provider Act and the Royal Decree of 6 December 2002 on the organization of the monitoring and accreditation of certification providers that provide qualified certificates (*Moniteur belge* 17 January 2003).

[20] Nicole Verheyden-Jeanmart, Droit de la Preuve, Bruxelles, Larcier, 1991, no. 357; Dominique Mougenot, *Droit des Obligations*. La Preuve, Bruxelles, Larcier, 2002, no. 63.

[21] See below.

[22] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce) (*Official Journal of the European Communities* No L 178 of 17 February 2000, pp. 1-16.

[23] Law of 11 March 2003 (*Moniteur belge* 17 March 2003).

[24] Patrick Van Eecke, "Artikelsgewijze Bespreking van de Wetten Elektronische Handel", in Patrick Van Eecke and Jos Dumortier (eds.), *Elektronische Handel*, Bruges, Die Keure, 2003, 12-16.

[25] Evelyne Terryn, "Nieuwe Informatieplichten voor de Dienstverlener", in Patrick Van Eecke and Jos Dumortier (eds.), *Elektronische Handel*, Bruges, Die Keure, 2003, 58.

[26] When these requirements were laid down in the law, the "postal services" only referred to services provided by the Post, a government service. Since that time, the market for postal services has been liberalized to a great extent.

[27] Art. 17 of the Consumer Credit Protection Act (*Moniteur belge* 9 July 1991) states, "The contract comes into effect through the signing of the offer".

[28] Royal Decree of 9 June 1999 transposing directive 97/67/EC on common rules for the development of the internal market of Community postal services and the improvement of quality of service (*Moniteur belge* 18 August 1999).

[29] *Certipost* includes a platform for secure electronic communication http://www.certipost.be.

[30] Art. 31 of the Electronic Commerce Act.

[31] This means that a consensus on this matter must be reached in a plenary session of the Council of Ministers, in contrast to a normal royal decree, what can be enacted by just one minister.

[32] Article 1317 of the Belgian Civil Code.

[33] Law of 17 July 1975 on company accounts (*Moniteur belge*, 4 September 1975).

[34] Royal Decree of 12 September 1983 on the implementation of the law of 17 July 1975 on company accounts (*Moniteur belge* 28 September 1983).

[35] Article 8 of the Accounting Decree.

[36] One possibility is the use of WORM (write once, read many) storage devices, such as a CD-ROM or WORM diskette. These media guarantee that entries will not be modified or reversed in the same way as paper does, if not better. Software can also be designed in such a way as to make changes impossible.

[37] Article 8 of the Accounting Decree.

[38] Article 9 of the Accounting Decree.

[39] Art. 6 of the Accounting Act.

[40] Article 315, par. 3 of the Income Tax Code.

[41] Art. 14 §2 of Royal Decree no 1 of 29 December 1992.

[42] For VAT, since 1 January 1993; for income tax, since 16 July 1994.

[43] Article 315bis, par. 2 of the Income Tax Code and article 61 §1, par. 2 of the VAT Act.

[44] Question Time, House of Representatives, 27 April 1992 no 7, Question no 62, Coveliers.

[45] Commentary on the Income Tax Code 315/19-315/22, Commentary on the VAT Act 60/31-60/43 and ET 82752, available at http://fisconet.fgov.be. The tax authorities also use this technique to resolve their storage problems. Art. 37 of the law of 7 December 1988 on the income tax reform and changes to taxes equivalent to stamp taxes stipulates that micro cards and microfilms of the registers have the same evidentiary value as the originals when they have been prepared by or at the behest of the income tax authorities.

[46] Cf. above: the central ledger, the integral journal, the three journals and the inventory ledger.

[47] This obligation is included in article 53, par. 1, 2) of the Belgian VAT Act.

[48] Study on the Requirements Imposed by the Member States, for the Purpose of Charging Taxes, for Invoices Produced by Electronic or Other Means, PricewaterhouseCoopers, Final Report, 23 August 1999.

[49] Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernizing and harmonizing the conditions laid down for invoicing in respect of value added tax, *Official Journal of the European Communities*, L 15/24, 17.1.2002.

[50] Art. 53 §2 Belgian VAT Act.

[51] Art. 1 §2 of Royal Decree no 1 of 29 December 1992 (*Moniteur belge* 31 December 1992).

[52] Art. 1 §3 of Royal Decree no 1 of 29 December 1992 (*Moniteur belge* 31 December 1992).

[53] Art. 1 §3 of Royal Decree no 1 summarizes the conditions in the definition of the advanced electronic signature found in the law of 9 July 2001 (*Moniteur belge* 29 September 2001). The differing terminology originates in Directive 2001/115, which also explicitly refers to the concept advanced electronic signature in art. 2, par. 2 of Directive 1999/93.It is regrettable that the King included the erroneous translation from the Directive in Belgian legislation. The French version of both the directive and the Royal Decree consistently use the term "signature électronique avancée".

[54] Art. 22, par. 3 b) Directive 77/388/EEC as emended by Directive 2001/115/EG.

[55] Axel Smits, Ine Lejeune, e.a., *Elektronische Facturering en Archivering in 20 Europese Landen*, Gent, Larcier, 2004, no. 391.

[56] Axel Smits, Ine Lejeune, e.a., *Elektronische Facturering en Archivering in 20 Europese Landen*, Gent, Larcier, 2004, no. 394-403.

[57] Art. 8 of Royal Decree no 1 of 29 December 1992 (*Moniteur belge* 31 December 1992).

[58] Art. 60 §3, par. 1 of the Belgian VAT Act.

[59] This involves administrative co-operation agreements of similar tenor to Directives 76/308/EEC and 77/799/EEC and (EEC) Ordinance no 218/92, art. 22 par 3d) clause 6, Directive 77/388/EEC, as is modified by Directive 2001/115/EC. See also I. Lejeune, S. Beelen and J.-M. Cambien, "BTW en het Elektronisch Bewaren van Facturen – de Grote Sprong Voorwaarts?", in *Computerrecht*, 2004, 18.

[60] Art. 60 §3, par. 3 of the Belgian VAT Act.

[61] Art. 60 §3, par. 2 and 3 of the Belgian VAT Act.

[62] Article 98 of the Belgian Corporation Law Code.

[63] The complete scheme applies to large companies, the abbreviated scheme to small businesses. Whether a company is to be considered large depends on whether or not it has exceeded the size criteria described in art. 15 of the Corporation Law Code. Companies carrying out activities of a special nature that require a specific form of financial statement (such as credit institutions, insurance companies and holding companies) are required to submit their statements in paper form.

[64] Art. 177 of the Royal Decree of 30 January 2001 on the implementation of the Corporation Law Code (*Moniteur belge* 6 February 2001).

[65] Up to 1 April 2003 the electronic submission of financial statements was accepted in BEF, art. 177 §2 par. 3 of the Royal Decree of 30 January 2001.

[66] See http://www.balanscentrale.be/BA/E/P1_7.htm#Specific%20regulations%20for%20filing%20on%20floppy%20disk.

[67] See http://www.balanscentrale.be/BA/E/P4_1.htm.

[68] Art. 177 of the Royal Decree of 30 January 2001.

[69] Art. 178 of the Royal Decree of 30 January 2001.

[70] Art. 4-10 of the Royal Decree of 8 August 1980 on maintaining social documents (*Moniteur belge* 27 August 1980).

[71] Art. 11 of the Royal Decree of 8 August 1980 on maintaining social documents (*Moniteur belge* 27 August 1980).

[72] Art. 13-21 of the Royal Decree of 8 August 1980 on maintaining social documents (*Moniteur belge* 27 August 1980).

[73] Art. 105 of the Law of 2 August 2002 (*Moniteur belge* 29 August 2002).

[74] Art. 6 of the Royal Decree of 23 October 1978 on mainaining social documents (*Moniteur belge* 2 December 1978).

[75] Royal Decree of 30 November 1983 establishing the rules for maintaining and storing an attendance register in the diamond industry (*Moniteur belge*, 22 December 1983).

[76] Royal Decree on maintaining an attendance register in the hospitality industry (*Moniteur belge*, 20 December 1997).

[77] Art. 1-5 of the Royal Decree of 9 July 2000 on seasonal and occasional work in the agricultural industry (*Moniteur belge* 18 July 2000).

[78] Royal Decree of 17 June 1994 on keeping an attendance register (*Moniteur belge* 25 June 1994).

[79] Royal Decree of 18 February 1983 establishing the modalities for maintaining and preserving social documents for recognized dockworkers (*Moniteur belge*, 17 March 1983).

[80] Art. 4 §4 of Royal Decree no 5 of 23 October 1978 on maintaining social documents (*Moniteur belge*, 2 December 1978).

[81] Law of 5 March 2002 on the transposition of the Directive on the Posting of Workers (*Moniteur belge* 13 March 2002) See Philip Braekmans, *De Sociale Documenten: van Personeelsregister tot Dimona*, Diegem, Ced. Samsom, 2002, 19-28.

[82] Art. 24 of the Royal Decree of 8 August 1980 on maintaining social documents (*Moniteur belge* 27 August 1980).

[83] Art 2 and 25 of the Royal Decree of 8 August 1980 on maintaining social documents (*Moniteur belge* 27 August 1980) and art 2 3) and 9 of the Royal Decree of 17 June 1994 on the keeping of an attendance register (*Moniteur belge* 25 June 1994).

[84] Law of 26 July 1996 on the modernization of the social security system and the protection of the maintainability of the legal pension systems (*Moniteur belge* 1 August 1996).

[85] Royal Decree of 22 February 1998 introducing an immediate notification of employment, in application of article 38 of the law of 26 July 1996 on the modernization of the social security system and protection of the maintability of the legal pension systems (Moniteur belge 18 March 1998).

[86] George Carlens, "De Elektronische Aangifte van een Sociaal Risico (ASR) in de Sector van de Werkloosheidsverzekering", in *BTSZ* 2000, 1209-1243.

[87] See http://www.onssrszlss.fgov.be/onssrsz/index.htm.

[88] Art 69-71 of the program law of 30 December 2001 (*Moniteur belge* 31 December 2001) and the Royal Decree of 20 November 2002 (*Moniteur belge* 29 November 2002).

[89] Art. 105 of the Law of 3 July 1978 on employment contracts (*Moniteur belge* 22 August 1978).

[90] Art. 157-159 of the program law of 22 December 1989 (*Moniteur belge* 30 December 1989).

[91] Royal Decree of 8 March 1990 on the monitoring of divergences from the normal work schedule of part-time employees (*Moniteur belge* 16 March 1990).

[92] Art. 160ff of the program law of 22 December 1989 (*Moniteur belge*, 30 December 1989).

[93] Art. 146sexies and annex VIII of the General Regulations for the Protection of Labor, dated 11 February 1946 (*Moniteur belge* 3 April 1946).

[94] Here the legislator makes no distinction between an electronically or manually maintained medical file.

[95] SCHUTYSER, K., "Eigendomsrechten en Medische Dossiers", in *Rechtskundig Weekblad*, 1983-1984, 3023, no 2.

[96] Art. 38 to 47 of the Code of Medical Ethics, drafted by the National Council of the Belgian Medical Association, available from http://www.ordomedic.be.

[97] According to a study carried out in 1992 in the area around Kortrijk, 57.3% of the doctors used a computer to process their medical files. CALLENS, S., *Goed geregeld? Het gebruik van medische gegevens voor onderzoek*, Antwerp, Maklu, 1995, 202.

[98] Art. 1 §3.

[99] Art. 46 of the Code of Medical Ethics.

[100] Art. 2262 §1 a1. 1 Belgian Civil Code. See CALLENS and BRILLON, *La Conservation du dossier patient*, A study ordered by the Telematics Standardization Commission For Health Care, available from http://www.health.fgov.be/telematics/cnst/library.html.

[101] Art. 26 Precursory Title of the Belgian Rules of Criminal Procedure.

[102] HELMER, F.M.M., "Bewaartermijnen van Medische Dossiers", in *Nederlands Tijdschrift voor Medische Administratie*, volume 25, no. 96.

[103] Royal Decree of 3 May 1999 on the General Medical File (*Moniteur belge* 17 July 1999). The Royal Decree equates the general medical file with the comprehensive medical file as referred to in the National Institute of Sickness and Invalidity Insurance (RIZIV) regulations.

[104] Royal Decree of 3 May 1999 (*Moniteur belge* 30 July 1999).

[105] Telematics Commission, "Langetermijnbewaring van patiëntendossiers in ziekenhuizen" ["Long-Term Storage of Patient Files in Hospitals"], Recommendation no 7, available at http://www.health.fgov.be/telematics.

[106] Telematics Commission, Recommendations no 3 "Messages relating to the Electronic Medical Prescription (General)", no 4 "Electronic Health Care Messages", no 5 "Codification System for the Classification of Illnesses" and no 6 "The Electronic Message "Medical Prescription Addressed for the Pharmacist" (Part 1)" available at http://www.health.fgov.be/telematics.

[107] Art. 7 §2 j) of the Privacy Act.

[108] Art. 10 of the Patients' Rights Act.

[109] For a detailed discussion of the Act, see: DIRK DE BOT, *Verwerking van Persoonsgegevens*, Antwerp, Kluwer, 2001, 403 p.

[110] Art. 3bis 1° Privacy Act.

[111] Art. 1 §4 of the Privacy Act.

[112] Art. 1 §5 of the Privacy Act.

[113] Art. 1 §1 of the Privacy Act.

[114] Art. 1 §2 of the Privacy Act.

[115] Art. 3 §1 of the Privacy Act.

[116] These include the Belgian State Security Service, the Belgian Military Intelligence Service, Belgian National Security Authority as well as the security officers, the Permanent Supervisory Committee and the Investigatory Department of the Belgian Intelligence Service, insofar as the processing is required in the exercise of their assignments.

[117] Art. 3 §§4-7 of the Privacy Act.

[118] Art. 5 a of the Privacy Act.

[119] Art. 5 b of the Privacy Act.

[120] Art. 5 c of the Privacy Act.

[121] Art. 5 f of the Privacy Act.

[122] Art. 4 §1 2° of the Privacy Act.

[123] Royal Decree of 13 February 2001 implementing the Privacy Act hereinafter referred to as the "Privacy Decree" (*Moniteur belge* 13 March 2001), http://privacy.fgov.be/normatieve_teksten.htm.

[124] Art. 4 §1 3° of the Privacy Act.

[125] Art. 4 §1 4° of the Privacy Act.

[126] Art. 4 §1 5° of the Privacy Act.

[127] Art. 9 §1 of the Privacy Act.

[128] Art. 9 §1 par. 1 and §2 par. 1 of the Privacy Act.

[129] This refers specifically to a law, decree, ordinance, royal decree or a ministerial order.

[130] Art. 9 §2 par. 2 b) of the Privacy Act.

[131] Art. 9 §2 par. 2 a) of the Privacy Act.

[132] Art. 30 of the Privacy Decree.

[133] Art. 10 §1 a) of the Privacy Act.

[134] Art. 10 §1 b) of the Privacy Act.

[135] The doctrine on abuse of right can be applied here. See D. DE BOT, *Verwerking van Persoonsgegevens*, Antwerp, Kluwer, 2001, 227-228.

[136] Art. 10 of the Privacy Act and art. 32 of the Privacy Decree.

[137] Art. 3 of the Privacy Act.

[138] Art. 13 of the Privacy Act.

[139] Art. 12 §1 par. 1 and 5 of the Privacy Act.

[140] See D. DE BOT, *Verwerking van Persoonsgegevens*, Antwerp, Kluwer, 2001, 227-228.

[141] Art. 12 of the Privacy Act and art. 32-33 of the Privacy Decree.

[142] Art. 3 of the Privacy Act.

[143] Art. 13 of the Privacy Act.

[144] Art. 12 of the Privacy Act.

[145] Art. 12 §1 par. 3 of the Privacy Act.

[146] Art. 34-36 of the Privacy Decree.

[147] Art. 5 b) and c) of the Privacy Act.

[148] Art. 12 of the Privacy Act and art. 32-35 of the Privacy Decree.

[149] Art. 3 of the Privacy Act.

[150] Art. 13 of the Privacy Act.

[151] Art. 14 and 31 of the Privacy Act.

[152] Art. 6-8 of the Privacy Act.

[153] Art. 25-27 of the Privacy Decree.

[154] Art. 6 §1 of the Privacy Act.

[155] Art. 6 §2 of the Privacy Act.

[156] Art. 6 §2 1) of the Privacy Act.

[157] Art. 7 §1 of the Privacy Act.

[158] See D. DE BOT, *Verwerking van Persoonsgegevens*, Antwerp, Kluwer, 2001, p. 154.

[159] Art. 7 §2 of the Privacy Act.

[160] Art. 7 §2 e) of the Privacy Act.

[161] Art. 7 §4 of the Privacy Act.

[162] Art. 7 §5 of the Privacy Act.

[163] Art. 10 §2 of the Privacy Act.

[164] Art. 9 §2 of the law of 22 August 2002 on patient's rights (*Moniteur belge* 26 September 2002).

[165] Art. 8 §1 of the Privacy Act.

[166] Art. 8 §2 of the Privacy Act.

[167] Art. 8 §2 b) of the Privacy Act.

[168] Chapter II of the Privacy Decree.

[169] Art. 17 of the Privacy Act.

[170] Art. 17 §8 of the Privacy Act.

[171] Art. 51-62 of the Privacy Decree.

[172] Art. 31bis of the Privacy Act.

[173] Art 37 of the law of 15 January 1990 establishing and organizing the Crossroads Bank for Social Security (*Moniteur belge* 22 February 1990).

[174] Art. 36bis of the Privacy Act.

[175] For a discussion of the sectoral committees, see D. DE BOT, "De Commissie voor de Bescherming van de Persoonlijke Levenssfeer: "Tussen Droom en Daad Staan er Niet Alleen Wetten in de Weg, maar vooral Praktische Problemen"", in T.B.B.R., 2003, 6, 384-402.

[176] Art. 16 §1 of the Privacy Act.

[177] Art. 16 §2 of the Privacy Act.

[178] Art. 16 §1 of the Privacy Act.

[179] Art. 21-22 of the Privacy Act.

[180] Art. 22 a1. 1 of the Privacy Act.

[181] Art. 22 a1. 2 of the Privacy Act.

[182] Art. 41 of the Privacy Act.

[183] For an extensive overview, see: FILIP BOUDREZ, HANNELORE DEKEYSER and SOFIE VAN DEN EYNDE, *Archiveren van E-mail*, 2e rev. ed., Antwerp/Leuven, Antwerp Municipal Archives/ICRI K.U.Leuven, 2003, p. 27ff., can be consulted at http://www.antwerpen.be/david/.

[184] Art. 29 Constitution.

[185] Art. 259bis and 314bis of the Belgian Criminal Code.

[186] "Knowingly and willingly" is a term used in criminal law. It means that the person committing the crime was aware of the fact that he was committing a crime (the maxim "everyone is presupposed to know the law" plays a role here) and that, knowing quite well what he does, he wants to commit the offence.

[187] HENDRICKX, F., *op. cit.*, 190 and 195.

[188] Art. 109terD of the law of 21 March 1991 on the reform of some public enterprises (Telecommunication Act), *Moniteur belge* 27 March 1991.

[189] Art. 109terE 1° of the Telecommunications Act.

[190] Art. 88bis of the Belgian Code of Criminal Procedure Code.

[191] DUMORTIER, J., "Little Brother is Watching You: Mag de Werkgever het Internetgebruik van zijn Werknemers Controleren?", in *Liber Amicorum Roger Blanpain*, 1998, Die Keure, Bruges, p. 254-255; HENDRICKX, F., *Privacy en Arbeidsrecht*, Bruges, Die Keure, 1999, p. 198ff.

[192] Art. 17 2° of the Employment Contract Act (AOW).

[193] Collective Labor Agreement no 81 of 26 April 2002 on the supervision of the use of internet and e-mail at work and the protection of employees' personal privacy, declared binding by the Royal Decree of 12 June 2002 (*Moniteur belge* 29 June 2002).

[194] For a general discussion on this topic, see HANNELORE DEKEYSER, "C.A.O. nr. 81 tot Bescherming van de Persoonlijke Levenssfeer ten opzichte van de Controle op de Elektronische On-linecommunicatiegegevens" in X., *Mediarecht*, Brussels, Kluwer, loose leaf.

[195] For instance, time sent, sender, addressee(s), attachments, and reference to an answer to the message.

[196] Art. 9 of CLA no 81.

[197] A more sophisticated method consists in adding an extra field to each e-mail in which the employee must enter a file number or a classification code. This information immediately situates the e-mail in its context.

[198] Art. 16 of CLA no 81.

[199] For an explanation of the other neighboring rights, the reader is referred to the available legal literature, i.e. FABIENNE BRISON, "Naburige Rechten", in FRANK GOTZEN (ed.), *Belgisch Auteursrecht van Oud naar Nieuw*, Brussels, Bruylant, 1996, pp. 349-383; ALAIN BERENBOOM, *Le nouveau droit d auteur et les droits voisins*, 2nd ed., Brussels, Larcier, 1997, 503 p.

[200] See: HANNELORE DEKEYSER, *Digitale Archivering: een juridische stand van zaken vanuit Belgisch perspectief*, Deel 2: *Auteursrecht, Technische Beschermingsmaatregelen en Wettelijk Depot*, Antwerp Municipal Archive/ICRI, Antwerp/Leuven, 2003, p. 16ff, available at http://www.antwerpen.be/david.

[201] For an overview of common modes of exploitation see: JEAN-PAUL TRIAILLE and ALAIN STROWEL, *Le droit d auteur du logiciel au multimédia*, Brussels, Bruylant, 1997, p. 67.

[202] Art. 3 §1 and 2 of the Copyright Act.

[203] Art. 3 §3 of the Copyright Act.

[204] Art. 80, par 1 and 2 of the Copyright Act.

[205] See: Brussels 19 February 1997, *Revue de Droit Intellectuel: l'ingénieur-Conseil*. 1997, 107; Antwerp (9th chamber.) 28 February 2002, *Auteurs en Media 2002*, 4, 340. LOUIS VAN BUNNEN, "Procédure Pénale et Civile (L'Action en Contrefaçon)", in FRANK GOTZEN (ed.), *Belgisch Recht van Oud naar Nieuw*, Brussels, Bruylant, 1996, 401-424.

[206] Art. 80, par 4 of the Copyright Act.

[207] Fines must always be multiplied by a factor to take inflation into account. The conversion of fines into euros was regulated in the law of 26 June 2000 (*Moniteur belge* 29 July 2000). See: http://www.just.fgov.be The Judiciary and the Euro.

[208] Art. 1481ff of the Judicial Code.

[209] Art. 587 par 1, no 7 of the Judicial Code and art. 87, §1 of the Copyright Act.

[210] Art. 87 §2 of the Copyright Act.

[211] COM (88) 816 final, O.J. C. 12 April 1989, no 91, 9.

[212] Art. 10 of the Software (Protection) Act.

[213] Fines must always be multiplied by a factor to take inflation into account. The conversion of fines into euros was regulated in the law of 26 June 2000 (*Moniteur belge* 29 July 2000). See also: http://www.just.fgov.be The Judiciary and the Euro.

[214] BUYDENS, MIREILLE, *Auteursrechten en Internet, Problemen en Oplossingen voor het Creëren van een Online Databank met Beelden en/of Tekst*, Brussels, DWTC, 1998, 50-51.

[215] Art. 2, 5 of the Belgian Database Protection Act of 31 August 1998 (*Moniteur belge* 14 November 1998).

[216] A producer is established in the EU when he/she is a citizen of a member State or has his/her normal residence in a Member State. A company is established in the EU when the company is established according to the legislation of a member State and when the registered office, the central administration or the main establishment is located in the Union. If the company only has its registered office within the territory of the Union, its activities must have an essential and durable bond with the economy of a Member State. Art. 12 of the Database Protection Act.

[217] Art. 3, par. 1 of the Database Protection Act.

[218] Art. 2, 2 of the Database ProtectionAct.

[219] Art. 2, 3 of the Database Protection Act.

[220] One example is when one would provide access to information from someone else's database on one's own portal site. The users of the portal site would only request a limited amount of data from the database (non-substantial part). Yet this harms the producer's legitimate interests because users do not visit his/her site directly and see the advertising there.

[221] Art. 13 of the Database Protection Act.

[222] Art. 14 of the Database Protection Act.

[223] Art. 15 of the Database Protection Act.

[224] See above.

[225] www.gnu.org.

[226] www.creativecommons.org.

[227] See: HANNELORE DEKEYSER, *Digitale Archivering: een juridische stand van zaken vanuit Belgisch perspectief*, Deel 2: *Auteursrecht, Technische Beschermingsmaatregelen en Wettelijk Depot*, Antwerp Municipal Archive/ICRI, Antwerp/Leuven, 2003, p. 27ff, available at http://www.antwerpen.be/david/. See also: HANNELORE DEKEYSER, CHRISTOPH DE PRETER "De Totstandkoming en de Draagwijdte van Open Source-Licenties", in *Computerrecht*, 2004, pp. 216-220.

[228] This is also called Public Key Cryptography (as opposed to Private Key Cryptography), because it uses one key that is known to everyone and hence is public.

[229] For instance: http://www.thawte.com, http://www.globalsign.com, http://www.certipost.be.

REFERENCES PART 2

[1] INTERPARES 1, How to preserve authentic electronic records?, 2001; K. THIBODEAU, R. MOORE EN C. BARU, Persistent Object Preservation: Advanced Computing Infrastructure for Digital Preservation, in: Proceedings of the DLM-Forum on electronic records. European citizens and electronic information: the memory of the information society, Brussels 18-19 October 1999, Brussels, 2000, p. 113-118. (http://europa.eu.int/ISPO/dlm/fulltext/full_thib_en.htm).

[2] K. THIBODEAU, Building the Archives of the Future. Advances in Preserving Electronic Records at the National Archives and Records Administration, in: D-Lib Magazine (February 2001) Volume 7.

[3] The documentary form is the primary means by which the content of a record, its immediate administrative and documentary context, and its authority are communicated. (INTERPARES 1, *The InterPARES Glossary*, p. 3).

[4] J. ROTHENBERG en T. BIKSON, Digital Preservation. Carrying Authentic, Understandable and Usable Documents Through Time, Den Haag, 1999, p. 7.

[5] ICA, Guide for managing electronic records from an archival perspective, Parijs, 1997, p. 22.

[6] INTERPARES 1, Authenticity Task Force Report, p. 2.

[7] F. BOUDREZ, The digital recordkeeping system: Management inventory, information layers and decision-making model as point of departure, Antwerp, 2001; K. THIBODEAU, Overview of technological approaches to digital preservation and challenges in coming years, in: The State of Digital Preservation: An International Perspective, 2002, p. 4-31, (http://www.clir.org/pubs/reports/pub107/thibodeau.html); TESTBED DIGITALE BEWARING, Migratie: context and current status, Den Haag, 2001, (http://www.digitaleduurzaamheid.nl).

[8] J. ROTHENBERG EN T. BIKSON, Digital preservation: Carrying authentic, understandable and usable digital records through time. Report to the Dutch National Archives. and Ministry of the Interior, 1999 (http://www.digitaleduurzaamheid.nl/bibliotheek/docs/final-report_4.pdf); J. ROTHENBERG, An experiment in using emulation to preserve digital publications, Den Haag, 2000 (http://www.kb.nl/coop/nedlib/results/emulationpreservationreport.pdf); J. ROTHENBERG, Avoiding technological quicksand: Finding a viable technical foundation for digital preservation. A report to the Council on Library and Information Resources, Washington, 1999 (http://www.clir.org/pubs/reports/rothenberg/pub77.pdf); J. ROTHENBERG, Ensuring the longevity of digital information, Santa Monica, 1999 (http://www.clir.org/pubs/archives/ensuring.pdf).

[9] http://www.archivebuilders.com/aba010.html.

[10] http://www.rlg.org/preserv/diginews/diginews5-3.html#feature2.

[11] http://www.rlg.org/preserv/diginews/diginews5-4.html#feature2.

[12] This view is inspired on the "Migration on request" strategy of the CAMiLEON-project, and on the approach of the National Archives of Australia (P. MELLOR, P. WHEATLEY EN D. SERGEANT, *Migration on Request - a practical technique for preservation*, http://www.si.umich.edu/CAMILEON/reports/mor/index.html; H. HESLOP, S. DAVIS EN A. WILSON, *National Archives Green Paper: An approach to the preservation of digital records*, Canberra, 2002, http://www.naa.gov.au/recordkeeping/er/digital_preservation/summary.html).

[13] Since 15 October 2002, Microsoft Corporation follows a formal Support Life Cycle policy. This policy includes guidelines for the availability of product support. (http://support.microsoft.com/default.aspx?scid=fh;nl;complifeport). As a consequence, no support will be available for MS Word 2002 after 30 June 2008.

[14] "The general rule is that the longevity of storage media is greater than the longevity of the storage media drives, and that the longevity of the drives is greater than that of the software". (C. DOLLAR, *Authentic electronic records: strategies for long-term access*, Chicago, 1999, p. 86).

[15] The Blue Book version of the OAIS model is available on: http://wwwclassic.ccsds.org/documents/pdf/CCSDS-650.0-B-1.pdf. Information about the standard and its application is available on: http://www.rlg.org/longterm/oais.html and http://www.erpanet.org (Copenhagen workshop).

[16] T. THOMASSEN, Een korte introductie in de archivistiek, in: P.J. HORSMAN, F.C.J. KETELAAR EN T.H.P.M. THOMASSEN, Naar een nieuw paradigma in de archivistiek, p. 11-20; K. THIBOUDEAU, Building the Archives of the Future, in: D-Lib Magazine, Febr. 2001 (vol. 7, no. 2).

[17] Model requirements for the management of electronic records, Brussel - Luxemburg, 2001, p. 21-25; DOD, Design criteria standard for electronic records management software applications (DoD 5015.2-STD), Washington, 2002 (second version).

[18] INTERPARES 1, Authenticity Task Force Report, p. 2.

[19] An example of such an XML document, including file metadata, is available on the DAVID website (http://www.antwerpen.be/david/website/nl/dossier_metadata.htm).

[20] An example of such an XML file list is available on the DAVID website (http://www.antwerpen.be/david/website/nl/xml_metadata.htm).

I.R.I.S.
Document to Knowledge™

Image Recognition
Integrated Systems Group S.A.
Professional Solutions

Rue du Bosquet 10
Parc Scientifique de Louvain-la-Neuve
1435 Mont Saint Guibert
Belgium
tel. +32 10 48 75 30
fax +32 10 48 75 40

www.irislink.com

Printing
Nevelland asbl

Artwork
www.graph-it.net