Amano Digital Time Stamp Service
e-timing
2004/05/24
14:12:51
CEST
Time Stamp Authority

Legal Aspects of Trusted Time Services in Europe

Research Paper

commissioned by

AMANO

authored by

Jos Dumortier
Hannelore Dekeyser
Mieke Loncke

K.U.Leuven
Interdisciplinary Centre for Law & ICT (ICRI)

K.U.Leuven – Interdisciplinary Centre for Law & Information Technology

The Interdisciplinary Centre for Law & Information Technology (ICRI) is a department of the Faculty of Law of the K.U.Leuven (University of Leuven, Belgium). ICRI is a research and consulting group in the domains of information technology law, communications law and legal information processing. The Centre is headed by Professor Jos Dumortier.

ICRI has 15 full-time and an equal number of part-time and freelance researchers of seven nationalities.

In the area of information technology law, ICRI performed the general legal study in the framework of the European IDA-program (European Commission, DG Enterprise), the study on legal aspects of electronic signatures used by the European Commission to prepare the European Directive 99/93/EC (European Commission, DG Market) the discussion paper on data protection and standardization (CEN/ISSS), the study preparing the review of the European electronic signatures Directive (DG Information Society), etc. ICRI has been active in the European Electronic Signatures Standardization Initiative (EESSI) and in the international research network in the field of digital archiving INTERPARES. In the area of geographical information systems ICRI is involved in the European Bridge-IT project. It also participated in the European CyberVote project (secure online voting). ICRI has been in charge of the legal part of the European RAPID roadmap in the area of privacy and identity management.

On the Belgian national level, ICRI has been intensively involved in a large number of e-government projects, such as the Belgian Electronic Identity Card, the modernization of the Civil Registry, IT-supported legislative process, secure exchange of XML-messages between public administrations, electronic long-term archiving, etc.

In the domain of communications law, ICRI carried out legal studies for several large telecommunications and cable operators, including Belgacom, BT, AT&T and others. ICRI worked also as a consultant of the Belgian Institute for Telecommunications and Postal Services preparing draft Belgian legislation in the framework of the transposition of the European regulatory framework on electronic communications.

ICRI has participated in several IT-projects e.g. for the Belgian Ministry of Justice (introduction of IT in courts and tribunals, automatic indexing of court decisions), Roularta (a leading Belgian publishing company – automatic abstracting of magazine articles) and the Federal Government (development of a legislative information system).

Table of Contents

1. What is, legally speaking, the right time?

The use of a standard time in society is a relatively recent phenomenon. Late into the 19th century, many towns and villages still set their clocks to local time based upon the position of the sun. The development of railways made this state of affairs untenable, as travellers were constantly required to adjust their clocks. After missing a train for just this reason in 1878, Sir Sandford Fleming invented standard time to fix the problem. Standard time divides the world into 24 'time zones', each one covering, in theory at least, 15 degrees. All clocks within each of these zones would be set to the same time.[1] Greenwich Mean Time, time measurement based on the Earth's rotation, was initially used to determine the standard time for each time zone. Since then several new ways of measuring time based on astronomical observations have been developed.

1.1. The International System of Units.

The International System of Units (SI)[2] was founded on May 20th 1875, when 17 nations signed the Convention of the Metre in Paris. Today there are fifty-one member states, among which all the major industrialized nations, and 18 associate members. The Metre Convention does not embody the standards for measurement units itself, but provides a permanent framework for member states to reach international agreement on all matters related to units of measurement. To this end, the convention constitutes three treaty bodies: the General Conference on Weights and Measures (*Conférence Générale des Poids et Mesures*, CGPM), the International Committee for Weights and Measures (*Comité International des Poids et Mesures,* CIPM*)* and the International Bureau for Weights and Measures (*Bureau International des Poids et Mesures,* BIPM).

The General Conference on Weights and Measures convenes in Paris every four years and reunites delegations from the member state governments as well as observers from the associate member. The CGPM is the highest authority within the Metre Convention and the final responsability for the development of the International System of Units is in its hands. Developments in the scientific world are followed

[1] <http://en.wikipedia.org/wiki/Universal_Time>

[2] The BIPM maintains a website with extensive information about the International System of Units at <http://www.bipm.org>.

closely and when appropriate the SI is adjusted to reflect fundamental new metrological findings. Decisions reached within the convention are released in the form of resolutions, which contain suggestions, requests and recommendations addressed to the member states. Although the resolutions do not have binding force, they carry considerable weight and are often incorporated into national law by the member states. The CGPM is also responsible for the organization of the BIPM.

The International Committee for Weights and Measures works under the authority of the CGPM. The CIPM is made up of eighteen members, each from a different member state, elected by the CGPM. The CIPM is charged with surveilling the uniform implementation of the units of measurement world-wide. Also, the CIPM prepares the CPGM meetings by submitting proposals and by issuing a report on the administrative and financial position of the BIPM. To help the CIPM with its task, several Consultative Committees were created, amongst which the Consultative Committee for Time and Frequency (CCTF).

The BIPM is responsible for the day-to-day administration of the SI. Its main mission is to ensure that a single coherent system of measurements is used that can be traced back to the SI. The BIPM is directly involved in the dissemination of the standard units of mass and time.[3] In other cases the BIPM coordinates the comparison of existing national measurement standards.

The Metre Convention and specifically the BIPM play an important role in the measurement of time. Untill 1956 the second was defined with reference to the rotation of the Earth where a second is 1/86.400 of a mean solar day. Research showed that the rotation was too unstable to serve as a reliable basis for precise time measurement. Under the mandate given by the 10th CGPM, the CIPM adopted a new definition of the second as it was formulated by the International Astronomical Union, where one second is "the fraction 1/31 556 925.9747 of the tropical year for 1900 January 0 at 12 hours ephemeris time". This decision was then ratified by the 11th CGPM in 1960. The development of atomic clocks soon afterwards prompted the 13th CGPM to revise the definition of a second again in 1967. Currently, the second is defined as "the duration of 9,192,631,770 periods of the radiation corresponding to the transition between the two hyperfine levels of the ground state of the cesium 133 atom".[4]

[3] The BIPM establishes and disseminates International Atomic Time (TAI) and Coordinated Universal Time (UTC).

[4] BIPM, *SI brochure*, 7th Ed., Paris, Organisation Intergouvernementale de la Convention de la Mètre, 1998, p. 95,

Once the definition of the atomic second was introduced, work began on a reference atomic time scale amongst others by the Bureau International de l'Heure (BIH). The CCTF[5] proposed a first definition of International Atomic Time in 1970: "International Atomic Time (TAI) is the time reference coordinate established by the Bureau International de l'Heure on the basis of the readings of atomic clocks operating in various establishments in accordance with the definition of the second, the unit of time of the International Systm of Units".[6] In 1971, the 14th CGPM requested the CIPM to give a definition of TAI and to to take the necessary steps, in agreement with the international organizations concerned, to create a realization of the International Atomic Time scale that satisfies the requirements of users. The responsability for TAI remained with the BIH[7] until 1988 when it was transferred to the CIPM. To calculate TAI, the BIPM performs a weighed comparison of about 200 atomic clocks maintained by the national time-service laboratories under metrological conditions. The result can be considered as a world reference time scale.

TAI has several uses in the scientific community, but is not distributed in this form for use in general society. The time-scale used in everyday life is Universal Coordinated Time (UTC), which differs from TAI by an integral number of seconds[8]. The lag is necessaryto take into account the irregularities in the rotation of the Earth, thus ensuring that the Sun is overhead on the meridian of Greenwich within 0,9 seconds of 12:00:00 UTC.[9] In this respect, UTC is considered the modern successor of Greenwich Mean Time (GMT). National time-service laboratories establish their own approximation of UTC, designated UTC(*k*) for laboratory *k*. In resolution 5 of the 15th CGPM the use of UTC is strongly recommended, considering that it is widely available by way of radio broadcast. This resolution has no legally binding force on member states, nonetheless UTC is widely used as legal time around the globe.

<http://www1.bipm.org/en/si/si_brochure/> Section 2.1.1.3.

[5] The CCTF was know as the Consultative Committee for the Definition of the Second (CCDS) at the time.

[6] BIPM, *SI brochure*, *o.c.*, p. 142, <http://www1.bipm.org/en/si/si_brochure/> Appendix 2, section 3.2.

[7] At that time the BIH was replaced by the International Earth Rotation Service, <http://www.iers.org>

[8] Leap seconds are added or subtracted upon the advice of the International Earth Rotation Service. <http://en.wikipedia.org/wiki/Coordinated_Universal_Time>

[9] BIPM, *SI brochure*, *o.c.*, p. 142, <http://www1.bipm.org/en/si/si_brochure/> Appendix 2, section 3.3.

1.1.1. Legal time

European Union

The Directive 2000/84 on summer-time arrangements[10] uses a wide variety of terms to refer to time measurement: 'universal time' in French, Portugese, Italian and Spanish; 'world time' in German and Dutch; 'Greenwich Mean Time' in English, Finnish and Swedish; 'UTC' in Danish. This inconcistency is higly regrettable and can only be attributed to the general terminological confusion in the field of time-keeping.

As this Directive only pertains to the beginning and end time of summer time, its weight in the discussion of the standard of legal time in the member states should not be exagerated.

Several countries in the EU explicitely refer to UTC in their legislation, amongst others France and Germany. Others, as the U.K. and Belgium use the term GMT. Due to the principle of free flow of goods and services in the internal market, restrictions based on the standard of time used in a service are not permissable as a rule. A German service provider that adheres to UTC may provide his services in the entire EU.

The ETSI technical standard 102 023 on policy requirements for time-stamping authorities (TSA's) specifically demands that the TSA synchronizes its clock with the UTC realization of a laboratory recognized by the BIPM.

Belgium

The law of April 29th, 1892 introduces Greenwich Mean Time as the legal time in Belgium. Two decrees of 1946 and 1947 set legal time ahead one hour of GMT in accordance with the Central European Time Zone. From 1977 onwards, “summer time” sets legal time ahead two hours of GMT for part of the year. By Royal Decree of December 19th, 2001 summer time was given a permanent character pursuent to the EU Directive 2000/84 on summer-time arrangements.[11]

The variety of terms used in all these regulations is remarkable and makes their interpretation all the more precarious. The Royal Decree on summer time alone refers to 'world time' in the Dutch language

[10] Directive 2000/84/EC of 19 January 2001 on summer-time arrangements, Official Journal L 031 , 02/02/2001 P. 0021 – 0022.

[11] M.B. December 28th, 2001.

version and to 'universal time' in the French language version. The law of 1892 clearly refers to Greenwich Mean Time, but should this term still be taken literaly today? In general language the concepts GMT and UTC are often used as synonyms.

Several arguments can be made against such a literal interpretation in favour of a more teleological one. The law of 1892 was written at a time when measuring time based on observations of the Earths rotation was the only available option. Since then much more accurate methods of time-keeping have been developed. The law never prescribed how GMT should be measured, thus in effect leaving this task up to the scientific community. According to the BIPM, UTC is the appropriate standard for time-keeping for civil purposes. The Royal Observatory for Belgium disseminates its realization of UTC in real-time to Belgian users, thus making UTC readily available to society. In 1970 the definition of the second as provided by the SI was incorporated into Belgian law. This definition, which is based on atomic time, is at odds with time-keeping based on the rotation of the Earth. Today the term GMT should be interpreted as “world time”, meaning the standard of timekeeping for civil purposes endorsed by the CGPM. Consequently, UTC should currently be regarded as legal time in Belgium.Precise time-keeping has clearly not been an issue in the legal world for over a hundred years. Since 1892 there has been no parliamentary debate on the subject in Belgium, nor are there any publicly known cases on the topic of legal time. The inconcise use of time-keeping terminology in all levels of government illustrates this point exactly. Until recently this state of affairs was perfectly reasonable, as civil society in general was not concerned with time measurement better then one second accurate.

The computer has changed all this, as it can perform many actions in well under a second. Therefor, it is no surprise that the issue of legal time has caught the attention of the government precisely in relation to cyber-crime. In 2000 existing criminal procedural law was amended to provide law enforcement agencies the power to monitor all modern types of telecommunication as well as the right to obtain certain information from telecommunication network operators. The government was mandated to provide detailed regulations by Royal Decree. The R.D. of January 9th, 2003 pertains to the obligations of telecommunication network operators to assist in criminal investigations. Amongst other data, the exact time of connection must be provided. Art. 8 provides that “the time indications must use the 24h time system and be precise to the second. The time indication must refer to the Belgian time zone, taking into account summer and winter time. Operators of telecommunication networks and telecommunication service providers must synchronize their system clock with the legal time-keeping system, in accordance with the conditions to be defined in a Ministerial Decree."[12] This article was inserted at the request of the Federal Computer Crime Unit, as knowing the exact time down to the second is crucial for criminal investigations in network environments. The notion 'legal time-keeping system' is a novelty and untill the M.D. clarifying its meaning is issued, this provision cannot be applied.

The government might implement their own time-keeping system for this purpose, but they could also opt to provide a framework for a market-based solution. The Royal Observatory of Belgium is already equiped to provide time services as it already delivers its realization of UTC to the BIPM. The ROB also broadcasts a time signal accessible via dial-up modem. Telecom network operators and service providers could be required to use this time signal, but it would be difficult to prove if they had actually done so afterwards as the ROB does not offer a monitoring service.

There are several arguments in favour of the framework approach. Criminal investigations are only one of the areas where the use legally recognized time is important. Other examples can be found in e-government applications, e.g. to determine the timeliness of the submission of a tax declaration, and in e-commerce, e.g. to determine the beginning and end time that the customer accessed a service. Moreover, imposing synchronization with a Belgian time-keeping service may be regarded as an impediment to internal market trade. Restrictions based on the standard of time used in a service are not permissable as a rule, due to the principle of free flow of goods and services in the internal market. A framework regulation would only describe the requirements to be met, without prescribing how to fulfill them. An obvious requirement would be that the service provider synchronizes its services with UTC or alternatively with the legal standard of time of the EU member state where it is located. A second requirement could be that the service provider must be able to prove that synchronization was performed succesfully.In order to eradicate any discussion on the notion of legal time in Belgium, the government should clarify that UTC is the current standard of time. The demand for legally recognized time services is bound to increase with the proliferation of electronic transactions with legal relevance. In the long run punctual legal reforms will not suffice to provide the legal certainty needed by citizens and businesses.

[12] Art. 8 of the R.D. of January 9th, 2003 (*M.B.* February 10th, 2003), available at <http://www.juridat.be/cgi_loi/wetgeving.pl> (Authors translation).

2. What is the legal value of a time-stamp?

In this research paper, the term 'time-stamp' refers to a digital certificate that contains the hash code of a referenced record and a time indication.[13] The certificate is signed by the Time Stamping Authority (TSA) by way of asymmetric encryption based on PKI, in other words a digital signature.[14]

Time-stamps may play different roles in a legal context. Their most straightforward use is of course to indicate the exact time of an event or action. The law frequently ties consequences to a certain date and time or the lapse of a period of time:

- The Civil Registry records the exact time of registration of some important events in the life of every citizen, such as birth, marriage or decease. Article 34 of the Belgian Civil Code states: "Acts of the Registrar's Office mention the year, day and time when they were drawn up, (…)".
- Article 1624 of the Belgian Civil Code provides that the risk of loss or damage is transferred onto the buyer at the time the sale is concluded. If the goods perish after the sale but before delivery, the buyer will not be reimbursed.
- In Belgian labour law, for instance, the immediate termination of an employment contract for urgent reasons, is valid under the condition that it occurs within a period of three working days after the date of the event that is invoked as the reason for the termination.
- The Judicial Code contains countless procedural deadlines that must be respected by all parties to a case and by the court itself.

The defining properties of time-stamps, namely the use of asymmetric encryption based on PKI and the use of trusted time, extend their usefulness beyond the mere indication of the time. Asymmetric encryption can be used to verify that an electronic record has not been tampered with in any way. On top of this, the trusted time indication certifies that the file existed at a certain point in time in a certain form. Thus, time-stamps can be regarded as software

[13] In general, the word time-stamp is used for any time indications that computer systems add to metadata of files or in system logs.

[14] The term electronic signature is used in the broader sense of any electronic authentication method.

alternative to WORM[15] media.

This chapter gives an overview of some key legal domains were time-stamps could play an important role.

2.1. Civil law

2.1.1. Contracts law

Legal rules enforcing the use of paper documents in the contractual process are progressively being abrogated. The European Directive 1999/93/EC [16] paved the way for electronic signatures. Furthermore, the Electronic Commerce Directive [17] obliges the member states to ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts, nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means. Consequently, a lot of important documents, that are now still mostly paper-based, such as contracts and other legal instruments, will in the future solely exist in their original electronic form.

The PKI-based technique of the digital signature plays an important role in this new legal framework. In the current state of affairs, only PKI-based digital signatures can fulfill all the conditions to produce "qualified" electronic signatures. The digital signature in the legal sense is used to authenticate electronic information in a way that the origin of the information, as well as its integrity can be verified. A digital signature is an encrypted hash-code that is deduced from and attached to the electronic information that has to be authenticated. If only one bit changes over time, the verifier of the digital signature will notice that the integrity has been affected. The verifier can also be sure that the electronic information originates form the signatory, since he is the only one who knows his own private key.

[15] Write Once Read Many, e.g. writable Compact Discs.

[16] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *Official Journal*, 19 January 2000, L13/12. <http://www.europa.eu.int/eur-lex/nl/index.html>

[17] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *Official Journal*, 17 July 2000, L 178/1. <http://www.europa.eu.int/eur-lex/nl/index.html>

The recipient of a digitally signed document is well advised to have it time-stamped as well. From a digital signature alone it is impossible to tell whether the document was signed within the time span allowed by the corresponding public key certificate. Time-stamping should happen as soon as possible after signing, as the certificate may be revoked or suspended at any time. Time-stamps, which are also based on PKI, guarantee the integrity of the record, while the time indication provides a time axis against which the signature can be evaluated.

In the long-term more measures must be taken to enable validation of both the digital signature and the time-stamp. Just preserving the electronic record, the signature file and the time-stamp itself is insufficient to enable validation years later. The certificates linking the public keys with their owner, the signatory and the TSA respectively, must be obtained. Furthermore, each certificates' validity at creation time of the signature and the time-stamp respectively must be proven as well. Each certificate has an expiration date and may be revoked or suspended at any time during its lifetime. Consequently, the certificate status information must be archived as well.[18] In essence, the certificate used to create the time-stamp must in its turn be time-stamped.

The long-term aspects of PKI have been studied in relation to the archival of digital signatures, as is explained in more detail in section 3.4.1. In view of the implementation of the Electronic Signatures Directive, the European Commission mandated the European standardization bodies, CEN/ISSS and ETSI, to analyse any further needs for standardization activities in support of the widespread adoption of electronic signatures. Under the auspices of the European ICT Standardization Board the European Electronic Signature Standardization Initiative (EESSI) was launched. The first result of this initiative was an expert report about future standardization requirements. This report affirms that trusted archival services could play an important role in supporting electronic signatures that may need to be used in evidence long after they were created and identifies it as a topic requiring further study since no standards exist yet for the use of such services in support of electronic signatures.[19] In the mean time, ETSI has published a standard

[18] It is the responsibility of each Certification Authority (CA) to make available in repositories on the Internet all the information needed to validate any signature that was created by means of a certificate issued by that CA. This includes making public at a regular basis information about the time a certificate expired, or was revoked or suspended.

[19] NILSSON, H., VAN EECKE, P., MEDINA, M., PINKAS, D. and POPE, N., European Electronic Signature Standardization Initiative, Final Report of the EESSI Expert

"Electronic Signature Formats" defining all the elements necessary to prove the validity of a signature long after the normal lifetime of the critical elements of an electronic signature.[20] All these elements form a so-called validation chain, that must to be archived in its entirety.

From the above it is clear that time-stamps are a valuable tool in the preservation of electronic records, on the condition that they are embedded in an overarching archival strategy. Time-stamps presuppose that the electronic record that it is applied to remains completely unchanged at the bit-level. Achieving this over extended periods of time is no simple feat from a technical point of view. Due to software and hardware obsolescence, preserving the original bit stream may even be pointless as the format of the file used may become unintelligible by future generations of computers. Migration to a new format is a favoured solution among experts to keep records accessible and legible. After migration, the original time-stamp can no longer be validated. Emulation of the native computer platform may one day provide a viable alternative, but the research in this area is still in a highly experimental phase. The archival of electronic records is a highly complex matter and will probably be entrusted to experts, so-called trusted archival service providers.

2.1.2. Evidence law

The rules of evidence established in the Civil Code have a general bearing and apply in any legal domain, unless more specific rules are provided. Evidence can be defined as "material establishing the accuracy of a fact or of the existence and content of a legal act, whenever a disagreement arises between several parties."

In principle, the evidence regime is free, which means that any legally obtained piece of evidence may be presented in court to prove a case. The judge enjoys sovereign authority to evaluate the trustworthiness and the value of the evidence before him. One condition is that the evidence upon which the judges bases his decision has been fully discussed by all parties.

The value of electronic records as evidence has been addressed by judges, not only civil cases but in criminal cases as well. In October 1995, the Court of first instance of Namur decided that turning to

Team, 20 July 2000, 69, available at: <http://www.ict.etsi.fr/eessi/Documents/Final-Report.pdf>

[20] Electronic Signature Formats, ETSI TS 101 733 v.1.3.1 (2002-02).

modern technology in order to obtain evidence is permissible. Such proof must be allowed when it is legally obtained and when there is no reason to suspect any falsification. It is up to the judge to evaluate the value of the evidence presented to him.

An exception to the general principle can be found in contracts law where strict rules apply concerning the kinds of evidence that are permissible. Only the kinds of proof listed in the law may be presented in court to prove the existence and extent of a contractual obligation. As a rule, contractual obligations may only be proven with a document signed by both parties or an authentic document. The law favours such forms of proof as signed documents are regarded as highly suited to identify the parties and ensure the integrity of the content.

Authentic documents are documents that have been drawn up by a notary according to specific legal formalities[21]. Such documents are considered highest in the hierarchy of evidence, as the law regards that all facts noted by the notary in person are incontestably proven.[22] The date and time of the document are notable examples of such facts. Due to the special qualities attributed to authentic documents, some parts of its content are binding proof with respect to third parties. Although they are not bound by its content, they cannot dispute the existence of the document.

Today, authentic documents can only be made in paper form, but this is bound to change sometime in the future. Time-stamping will prove equally important to authentic documents as for regular documents.

A contract, whether authentic or private, binds all signatories as if it were the law. The parties are free to determine the contract's terms and conditions as they see fit, unless the law says otherwise. If they agree to include a different date and time than the actual date and time, the one mentioned in the contract is regarded as the truth with respect to the signatories.[23] The method used to date the contract, manually or by time-stamping, is of no consequence. Third parties are in no way bound by the date mentioned in the contract. However, when time-stamps are used a contract's date may well carry more weight. As the restrictive rules of evidence only apply to the contracting parties, the date of a contract may proven or disproven by

[21] Other officials like the mayor or an official of the Registry Office are sometimes qualified to draw up authentic documents as well. These do not have the same evidence value as documents from a notary.

[22] The only exception is when the notary in question is prosecuted for forgery afterwards.

[23] Article 1320 of the Belgian civil code.

any available means in a dispute with a third party.

In general, the time and date of an event or transaction may be proven by any means available, as this is an element of fact. Sometimes, the law requires a contract or document to have a '*fixed date*'. The goal is to prevent conflicts from arising or to strengthen the position of certain parties. An example is the lease of goods or property. Article 1743 of the Belgian civil code states that, when the goods or the property are sold the new owner may not evict the tenant immediately if the latter has an authentic leasing contract or a contract with a fixed date[24]. A 'fixed date' makes the existence of the contract opposable to third parties. Article 1328 of the Belgian civil code enumerates three possibilities for private acts to obtain a 'fixed date':

-Through registration of the document at the registration office;

-When one of the signatories to the act has deceased;

-When the essence of the private act has been incorporated in an authentic document.

Registration is the cheapest way to give documents a fixed date. However, as of yet electronic documents cannot be submitted for registration. Time-stamps could append a fixed date to electronic documents and the law should be amended to include this option.

2.2. Commercial and economic law

2.2.1. E-commerce

E-commerce reunites the issues related to distance trading and the legal validity of electronic transactions. As is the case for all distance contracts, the parties to a contract concluded on line are located in different places or do not meet in person. The trustworthiness of the other party is more difficult to assess in such situations. Are they who they say they are? Where are they really located? Are the goods or services described accurately? The electronic environment compounds these issues, as the links between the on line business and the real world are often tenuous and fleeting.

[24] Unless the landlord has reserved the right to do so in the leasing agreement.

The EU Directive 2000/31 on e-commerce[25] has sought to deal with several problems related to on line commerce, amongst other the issue of trust. All providers of services related to the information society must keep certain information permanently accessible to the recipient of the service.[26] The data in question is on line and off line contact information, and where applicable trade registration number, licence number, professional title and VAT number. In case on line orders are accepted, the different technical steps to follow must be clearly indicated and the technical means to correct input errors prior the final placement of the order must be outlined. Contract terms and general conditions provided by the recipient must be made available in a way that allows the customer to store them.[27]

The service provider must be able to prove that he respects al the provisions of the law.[28] When a dispute arises, it may be very difficult to prove what the site's content was at any given time. Regular time-stamping of the websites content, or more precisely the code constituting the website, could offer an efficient and affordable solution to this problem.

More recently, the EU has adopted measures to regulate unsolicited commercial communications, often called 'spam' in colloquial language. Directive 2002/58 on privacy and electronic communications[29] only allows unsolicited commercial communications upon prior consent given by the intended recipient.[30] An exception is provided for communications sent to customers about the senders own similar products and services, in which case the recipient must be given the opportunity to opt out of the mailing list.[31] The sender must therefore prove that permission was obtained before sending the first communication or prove that recipient was already a customer. Again, time-stamps provide an efficient way to prove compliance with

[25] Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *Official Journal* L 178 , 17 July 2000 P. 0001 – 0016 or <http://www.europa.eu.int/eur-lex/nl/index.html>

[26] Art. 5 of the E-commerce Directive.

[27] Art. 10 of the E-commerce Directive.

[28] Art. 14 §4 of the Belgian E-commerce Act of March 11th, 2003 (*M.B.* March 17th, 2003) <http://www.juridat.be/cgi_loi/legislation.pl>

[29] Directive 2003/58 of the European Parliament and of the Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector. Official Journal L 201, 31 July 2002 p. 37-p.47 or <http://www.europa.eu.int/eur-lex/nl/index.html>

[30] Art. 13 §1 of the Directive on privacy and electronic communications.

[31] Art. 13 §2 of the Directive on privacy and electronic communications.

the law.

2.2.2. Internet Domain Names

The Internet Corporation for Assigned Names and Numbers (ICANN[32]) is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions.

Domain names can be registered through many different companies (known as 'registrars') that compete with one another. ICANN holds a list of companies that have been accredited to act as registrars in one or more TLDs.

As more companies move to put information and products onto the Internet, the clashes over Internet domain names become more common. Because of the increasing popularity of the Internet, companies have realized that having a domain name that is the same as their company name or the name of one of their products can be an extremely valuable part of establishing an Internet presence.

In order to guarantee a fair treatment and to avoid having to be the arbitrator between two parties who both desire the same domain name, they decided to simply adopt a 'first come, first serve' arrangement with respect to domain names. In the event that separate applicants submit registration requests for identical trademarks in the same registered name, the first request to be processed by the Registry Operator and successfully added to the zone file will be awarded the registration.

In case of disputes, the Rules for Uniform Domain Name Dispute Resolution Policy, as approved by ICANN on October 24, 1999, apply. It states the following:

"2.f Except as otherwise provided in these Rules, or decided by a Panel, all communications provided for under these Rules shall be deemed to have been made:

-if delivered by telecopy or facsimile transmission, on the date shown on the confirmation of transmission; or

-if by postal or courier service, on the date marked on the receipt;

[32] <http://www.icann.org>

or

-if via the Internet, on the date that the communication was transmitted, provided that the date of transmission is verifiable."

In this case, the proof of the exact time can clearly facilitate the battle to gain a certain domain name if a disagreement would arise later on.

2.2.3. Financial law

In Belgium, the prohibition on insider trading is regulated by the Financial Sector Act.[33] Insider knowledge is defined as: "Undisclosed information that is accurate and directly or indirectly relates to one or more issuers of financial instruments or to one or more financial instruments, and that has the ability, if disclosed, to influence the exchange rate of these financial instruments or the exchange rate of related financial instruments sensitively, (…)"[34]

According to the Belgian law, it is forbidden "to make use of insider knowledge to obtain or transfer or attempt to obtain or transfer, at one's own or someone else's expense, directly or indirectly, the financial instruments or related financial instruments where the prior knowledge refers to."[35] However, this prohibition doesn't apply to transactions performed in implementation of an obligation to obtain or transfer financial instruments in case this obligation has become due and arises from an agreement made before the said person even had the relevant insider knowledge.[36]

To prove a charge of insider trading against the investors concerned, the authorities must establish that they had prior knowledge of the impending stock changes to profit from investment actions. Documents indicating the exact time can prove or disprove the existence of insider knowledge someone's behalf.

[33] Act of August 2nd, 2002 on the financial sector and financial services, (*M.B.* September 4th, 2002) <http://www.juridat.be/cgi_loi/legislation.pl>.

[34] Art. 2, 14° of the Financial Sector Act. (Author's translation).

[35] Art. 25 §1 a) of the Financial Sector Act. (Author's translation).

[36] Art. 25 §2 of the Financial Sector Act. (Author's translation).

2.2.4. Accountancy law

The law of July 17th, 1975 on bookkeeping provides:
"Bookkeeping is done via a system of books and accounts taking into account the customary rules of double bookkeeping.
All transactions are entered in an undivided diary, without delay, faithfully, completely and chronologically, (…)"[37]

Article 8 of the same law reiterates: "The books are kept chronologically, without any blank spaces or any omissions. In case of correction, the original writing has to remain legible."

Accountancy law obviously attaches a great deal of importance to the unchangeable nature of bookings. Therefor, the main books must be made up in paper form. To prevent any tampering, all pages are signed in advance by a court clerk.[38] Time-stamps are much more sophisticated tool to ensure the unchangeable nature of the books as a whole or of each book entry seperately. Moreover, there would be no need to burden the courts with this task any longer, a private TSA would be able to provide this service.

2.3. Tax law

The levying of taxes by the tax administration generates a multitude of data streams in various directions. Both the administration and the tax-payer stand to benefit from the increased efficiency offered by electronic data exchange. Electronic invoicing is a prime example of this point, which is why companies have welcomed the harmonisation of invoicing procedures within the EU internal market.

Directive 2001/115 on the harmonisation of invoicing[39] provides that invoices may be issued in electronic form subject to acceptance by the customer. The member states must accept electronic invoices when the authenticity of the origin and integrity of the contents are

[37] Art. 4 of the law of July 17th, 1975 on bookkeeping, (*M.B.* September 4th, 1975) <http://www.juridat.be/cgi_loi/legislation.pl>.

[38] Art. 5 of the Royal Decree of September 12th, 1983 on bookkeeping, <http://www.juridat.be/cgi_loi/legislation.pl>.

[39] Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax, *Official Journal* L 015 , 17 January 2002, p. 24-28 or <http://www.europa.eu.int/eur-lex/nl/index.html>

guaranteed. The Directive mandates two methods of achieving this: the use of an advanced electronic signature, and the use of EDI. Optionally, member states may demand that a qualified signature is used. However, the notions advanced and qualified electronic signature are only used in a technical sense, as the Directive clearly states that the member states may not require invoices to be signed in a legal sense. The member states are free to accept other types of electronic invoices as they see fit.

Belgium has transposed the Directive into national law rather literally with respect to electronic invoicing. The VAT-code allows electronic invoices in principle, under the condition that the authenticity of the origin and the integrity of the contents are guaranteed.[40] Electronic invoicing is subject to acceptance by the customer. Advanced electronic signatures and EDI are both accepted means of electronic invoicing[41], as mandated by the Directive.

The Finance Minister may accept other means of electronic invoicing if the general conditions of authenticity and integrity are fulfilled.[42] This category of invoices is only legally valid in the countries that accept the electronic means used to issue them.

Are time-stamps suitable to create legally valid electronic invoices? Time-stamps are certificates containing a time indication and a hash value referencing a document, which are signed by the TSA using an advanced electronic signature. The time-stamp guarantees the integrity of the referenced document, in this case an invoice, from the time it was stamped. If the invoice is changed later, it will produce a new hash value that doesn't match the one contained in the time stamp. Any modification will therefor automatically be detected.

The fact that the TSA, a legal person, and not a physical person signs the time-stamp is irrelevant, as the notion electronic signature is used in a purely technical sense in this context.[43]

The question remains whether the time-stamp in itself guarantees the authenticity of the origin of the invoice. The signature used to create the time-stamp uniquely relates to the TSA, and not to the company issueing the invoice. At first glance, this appears to pose a problem. However, two general principles should be borne into mind in this

[40] Art. 53octies of the VAT Code

[41] Art. 1 §3 R.D. nr. 1 of December 29th, 1992.

[42] Art. 1 §4 R.D. nr. 1 of December 29th, 1992.

[43] CEN/ISSS report on standards and developments on electronic invoicing related to VAT Directive 2001/115/EC, p. 26, p. 43

respect. First of all the principle of technological neutrality holds that legal burdens should be the same regardless of the technology used. This is elaborated more concretely in the functional equivalence approach, as developed by UNCITRAL, which is based on analysis of the purposes and functions of the traditional paper-based requirement in order to find electronic ways to fulfill these purposes and functions.[44] In the traditional environment, the medium paper is relied upon to guarantee the integrity of invoices. The assumption being that it is hard to modify an existing paper document undetected. The authenticity of the invoice's origin is not guaranteed by the medium, but by the content of the invoice itself. The invoice must mention amongst other the issuance date, a unique identification number corresponding with the invoice register and the name and VAT number of the issuing company. An invoice is not an isolated document but is part of an audit trail, particulary by the use of a unique identification number linked to the company's books. With electronic invoices, time-stamps fulfill the function of paper, namely ensuring integrity. In this case, the content of the invoice is just as capable of ensuring the authenticity the origin in electronic as in paper form. The condition concerning the authenticity should therefor be deemed fulfilled.

Directive 2001/115 allows member states to determine the period of time that invoices must be stored and to some extent the place of storage. Member states may require that invoices are stored in their original form. In any case, the authenticity of the origin and integrity of the content of the invoices, as well as their readability, must be guaranteed throughout the storage period. Other obligations or formalities, e.g. use of a certain storage medium or format, may not be imposed.

According to the Belgian VAT code, invoices must be stored in their original form, paper or electronic, for a period of 10 years. The authenticity of the origin, the integrity of the content and the readability must be guaranteed for the entire storage period. Any data needed to ensure authenticity and integrity, e.g. a public key certificate, must be stored as well.[45]

The conditions indicated above do not pose any particular difficulties for time-stamped invoices. The integrity of a time-stamped invoice is maintained as long as the advanced electronic signature remains

[44] Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996), paragraph 15, <http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>. Doc. Parl. 50th session, 2100/01, p. 42-45

[45] New art. 60 §3 VAT code

reliable and the original bit-stream of the invoice remains intact. Readability depends on the file format used for the time-stamp and the invoice. The time-stamp is usually written in ASCII file format and will no doubt remain readable in the next decades, as ASCII is a well documented open standard. Appropriate measures must be taken to ensure that the file format of the invoice remains interpretable throughout the entire storage period as well.

The Belgian Tax administration is preparing an explanatory memorandum on electronic invoicing that will clarify the administrations views on this matter. A technical working group was founded, whose membership includes several bussinesses (Isabel, Certipost, Ubizen), the interest-group ICODIF and the administration. The memorandum is expected to be published within six months.

In conclusion, time-stamps are suited to create, exchangen and store electronic invoices in compliance with Belgian VAT-law.

2.4. Criminal and procedural law

Procedural law still largely relies on the use of paper, although there are signs even here the reign of paper will soon come to an and. Recently, electronic documents have been recognized as a valid form of notification within the scope of civil law procedures through the Act of October 20th, 2000.[46] The same law introduced the use of electronic documents in the Belgian Code of Judicial Procedure. Timely submission of documents is paramount in court proceedings and the law explicitly provides that the submission time of electronic documents is their time of arrival at the clerk's office.[47] In the near future, electronic submission of tenders will also be possible in the context of public procurement. In all these cases, disputes about the timeliness of submission can easily be avoided by time-stamping documents upon arrival.

Electronic information is increasingly being used by law enforcement agencies today not only as a distinct source of information but also as a means to increase efficiency. The use of digital surveillance camera's and wiretapping are two prime examples.

The use of video surveillance technology is commonplace today. Video

[46] Act of October 20th, 2000 (*M.B.* December 22nd, 2000). <http://www.juridat.be/cgi_loi/legislation.pl>

[47] New art. 52 of the Code of Judicial Procedure <http://www.juridat.be/cgi_loi/legislation.pl>

surveillance is used in banks and stores of all sizes in an attempt to reduce robberies, shoplifting and other crimes. It is also used to monitor public areas in casinos, sports arenas and parking lots. Law enforcement uses include undercover operations, emergency and disaster responses, media releases and crime scene recording. The home video camera can play a significant role, not only in television comedy shows, but occasionally in recording criminal behaviour. Video imagery of an incident has various potential uses. It can be used as leverage in an internal investigation or as evidence in court of law.

Jurisprudence in Belgium shows a growing acceptance of video images as evidence in court. In September 1997, the Labour Law Court of Antwerp decided that video images shot at publicly accessible places by a private detected with the sole intent of supporting the position of one party in legal proceedings and were not intended for publication and whose existence is communicated to the other party, should not be regarded as illegal and do not breach the right to privacy.

In March 2002, the Court of Appeal of Ghent concluded that the retrieval and the use of surveillance camera images by the police, gathered by the office of the National Bank of Kortrijk, produced valid evidence. Surveillance camera images of the public road can be regarded as permissible evidence and their use to demonstrate the existence of a crime of which the aforesaid bank is not the victim, does not constitute a breach of article 8 ECHR (privacy) nor of article 6 ECHR (fair trial)

The reliability of the video data is of the utmost importance since the data are of no use unless the time of the recordings as well as their authenticity can be established. Electronic documents will only stand up in court if the "who, what, and when" they represent are unassailable. In the U.K., where extensive use is made of video surveillance in law enforcement, the House of Lords Select Committee on Science and Technology published a report about the suitability of digital imagery as evidence in 1998.[48] The report recommends the use of authentication techniques, e.g. digital signatures and watermarks.

A correct time indication is not only important when video imagery is used directly to establish someone's guilt. The right time indication is also of key importance when information from different sources must be compared. For example, when log files from different devices on the network are collected in a single repository, time synchronization

[48] <http://www.parliament.the-stationery-office.co.uk/pa/ld199798/ldselect/ldsctech/064v/st0501.htm>

becomes an issue. The more devices on the network, the more difficult it is to keep them all synchronized. Without synchronized times, reporting will be confusing and unreliable. This was shown in the David Camm Case (United States – Indiana - 2002) where phone records were relied upon as an alibi. The phone records were regarded as objective evidence, giving the precise time. Weeks later, it was revealed there was an hour's difference between the actual time and the time indicated on the phone records. The mistake could be attributed to the fact that Indiana has two different time zones. The suspect's home is in one time zone, but his cell phone company's computers are in another time zone. A glitch in the company's computer resulted in an incorrect time on the bill.

The Belgian government has recognized the importance of synchronization in the Royal Decree January 9th, 2003 pertaining to the obligations of telecommunication network operators to assist in criminal investigations, as described previously. This decree demands that operators of telecommunication networks and telecommunication service providers synchronize their system clock with a legal time-keeping system.

Time-stamps are valuable tools to situate digital information in time and to ensure its integrity. Both these attributes are of key importance in criminal proceedings.

3. The Regulatory Framework for Time Services in Europe

The preceding chapters have been dealing with the legal status of "time" and with the role of time in a legal context. In the following pages we will focus our attention on the regulatory framework for time-stamping service providers in Europe.

3.1. Introduction

An inherent characteristic of electronic documents is that they can easily be modified. In a legal context security about the integrity of a document is in many circumstances an absolute necessity. Digital signature technology provides a means to verify the integrity of electronic data. It doesn't however provide the possibility to verify the time on which a document has been signed.

In the previous chapter we have seen that administrative and judicial procedures frequently necessitate a verification of the respect of deadlines. For example, if the conditions in a public procurement procedure state that bids have to be submitted on a certain date at the latest, every bid transmitted after 12 p.m. on that date will have to be considered as non-acceptable. Secure evidence that a deadline has been respected can only be delivered by a time stamp provided by a trustworthy service provider.

As described above, time stamping is also absolutely necessary in the context of electronic signatures based on the use of PKI. Such an electronic signature will only be valid if it is based on a certificate that has not expired or has not been suspended or revoked at the moment of signing. This can only be effectively verified if both the signatory and the revocation service use a secure time authentication.

Time-stamping services provide such a time authentication by delivering a digitally signed certificate stating that certain data have been submitted to the time-stamping authority at a certain point in time.[49]

[49] For a short introduction into time-stamping and time-stamping services, see A. Hartmann, Temporale Authentifikation und Zeitstempeldienste, Seminararbeit, 2001, <http://www.ifi.unizh.ch/ikm/Vorlesungen/Sem_Sich01/Hartmann.pdf>

3.2. Short history

The earliest legal documents dealing with digital time stamps have been published by the American Bar Association (ABA) in the context of the emergence of the first electronic signature laws in the US.[50] Particularly in the second half of the nineties, the ABA was very active in the discussion concerning the use of electronic signatures. The Guidelines published by the ABA have considerably influenced the initial discussions about digital signatures in Europe, particularly in Germany where the federal governement prepared the first "Signaturgesetz" (digital signature law) of 1997.

3.2.1. The ABA Guidelines

The ABA Digital Signature Guidelines published in 1996 introduce the subject of time-stamping by stating that "a digital signature, whether created by a subscriber to authenticate a message or by a certification authority to authenticate its certificate should be reliably time-stamped to allow the verifier to determine reliably whether the digital signature was created during the operational period stated in the certificate, which is a condition upon verifiability of a digital signature."[51]

"The operational period of a certificate begins on the date of issuance (or on a later date and time certain which is stated in the certificate) even though the certificate does not become valid unless and until acceptance by subscriber. This rule allows the certification authority to unambiguously fix the beginning of the operational period at time of issuance, without requiring reprocessing upon subsequent acceptance by the subscriber."

[50] ABA, Digital Signature Guidelines, Legal Infrastructure for Certification Authorities and Electronic Commerce, 1996. The document was drafted by the Information Security Committee, chaired by Michael Baum (Verisign).

[51] "A reliable time-stamp on the certificate also allows a determination as to whether it was created before or after the filing of a revocation or suspension of a certificate in a repository, which not only protects the subscriber who promptly revokes or suspends, but also provides increased assurance of nonrepudiatability by making it more difficult for a fraudulent subscriber to create a certificate and retroactively revoke it after reliance upon the certificate has occurred".

A further use might be the time-date stamping of historical versions of certification practice statements which have been incorporated by reference in the certificate, to determine which version was available to the subscriber and/or a relying party at pertinent times during the operational period of the certificate.

Among the requirements for time-stamping the ABA Guidelines also mention the following:

1. A time-stamp should be expressed in a form that clearly indicates its frame of reference so that time-stamps are universally comparable, notwithstanding different time zones and seasonal adjustments.

2. The probative value of a time-stamp will depend in part upon the extent to which the time-stamp is provided by a trustworthy system.

3. The design and implementation of a trustworthy system will differ depending on what the system is expected to do. For example, the trustworthy system required for a time-stamping service will differ in some respects from the trustworthy system required for a certification authority, since the services of time-stamping and of issuing certificates differ. For time-stamping, a trustworthy system would obviously need to include functionality for accurately determining the time and date, but might not require the key management functionality which is central to the operations of a certification authority.

Requirements for time-stamping, particularly in the context of records archiving have also been included in the **PKI Evaluation Guidelines** published by the ABA in 1998. The Evaluation Guidelines contain following interesting statements in relation to time-stamping:

Time stamping of records is a fundamental requirement of sound auditing and retention management practices. A time-stamp should be applied to and be inextricably linked with each archived record.

The time-stamp should be acquired from a source that is independent of the automated device (CAs server, subscriber's PC, etc.) that generated or is controlling the event - such as a third-party time-stamping service, or other automated device that is independent of the device (such as the subscriber's PC) that is generating or controlling the event (an independent "archive system server").

- Timestamping needs a certified or externally audited timebase; the goal of the timestamp is to fix an event in the temporal plain. To be effective at this requirement the user or consumer of the timestamp should have an arms-length from the time data , the timestamping process, and the non-repudiated logging that these technologies enable.

- Timestamp processes may also mandate the addition of certifiable location specific data to localize applicable jurisdiction.
- The timebase used in creating the time stamp should be acquired from a source of legally credible time data. That is to say a time data source from which a end-to-end chain of custody can be demonstrated for the time data itself. Also included in this time data is the authentication and source certification data or tokens.
- These timestamping resources may take the form of certified, locally or remotely operated or independent clocking systems such as those of an external timestamping service or archival services provider.
- The time-stamp as used to control retention management may vary based on when the record was: signed/received (chronological retention), when it became effective, or any other event that initiates the start of the retention period. If the record(s) is migrated or converted to another system and/or media, the originally assigned time-stamp must be preserved. Likewise, anytime the document is opened or resigned, it may require restamping.
  Likewise, when compromises in the underlying technologies occur, archival storage systems must address the requirement to restamp or modify the existing timestamps inline without destroying the original token validity.

3.2.2. The first German digital signature law

As mentioned before, the documents produced by the ABA and other organisations in the US – in particular the business model presented by the California-based company "Verisign" - have considerably influenced the drafting of the first electronic signature law in Europe, which was the German "Signaturgesetz" (digital signature law) of 1997.[52]

The German digital signature law stated in its first paragraph that the

[52] For the (German) text of the first Digital Signature Law, see: <http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/4.pdf>. There is an English translation available at: <http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/11.pdf>

purpose of the law was to "create general conditions under which digital signatures are deemed secure and forgeries of digital signatures or manipulation of signed data can be reliably ascertained". The law of 1997 established a very detailed framework, which was further developed in an Ordinance of 8 October 1997 and in a series of technical specifications.[53]

At the top of the administrative infrastructure, as an overall supervisory authority responsible for the granting of licenses to certification authorities, the issue of certificates used by those authorities for the signing of certificates and the monitoring of compliance with the act, the main responsibilities in this area were assigned to the "Regulierungsbehörde für Telekommunikation und Post", which functioned since the 1st of January 1998 as the regulatory authority for the German telecommunications sector.

Licenses were granted to certification authorities wishing to operate under the legal framework, after examination of their application file which had to include a security concept[54] in accordance with the security requirements of the law and after a check of the implementation of that security concept by a body recognised by the supervisory authority[55]. According to § 1(3) of the Ordinance the supervisory authority had to hear the applicant before rejecting, withdrawing or revoking a license. After the granting of the licence the supervisory authority issued the certificates for the signature keys used for affixing signatures to certificates and kept those certificates available for verification and retrieval over publicly available telecommunication links.

As a definition of "time-stamp", § 2(4) of the law stated:

"For the purposes of this Act "time stamp" shall mean a digital declaration bearing a digital signature and issued by a certification authority confirming that specific digital data were presented to it at a particular point in time."

[53] The technical specifications have first been established in a very detailed "catalogue" (the so-called "Massnahmenkatalog"). A simplified version has afterwards been included in the "BSI-Manual for Digital Signatures" (see later).

[54] The security concept shall include all security measures and, especially, an overview of the technical components used and a description of the procedures used in certification.

[55] Such a check has to be repeated "following security-relevant changes and at regular two-year intervals" (§ 15(1) of the Signaturverordnung).

Further in the law, § 9 provided: "Upon request the certification authority shall affix a time stamp to digital data. §5(5) sentences 1 and 2 shall apply accordingly".[56]

The Ordinance of 8 October 1997, which contained the further implementation measures of the Digital Signatures Act, stated in § 1 that, in order to obtain a license to provide time-stamping services "the applicant must prove that personnel involved in the certification procedure or in issuing time stamps have the necessary professional qualifications."

§ 4.1 of the Ordinance further mentioned: "The certification authority shall notify applicants concerning the following necessary measures to ensure the security of digital signatures:
(1) ...
(5)"If a particular time can be of considerable significance with regard to use of signed data, a time stamp shall be appended."

In § 11 the Ordinance also determined: "The certification authority shall take precautions to protect the following from unauthorised access: private signature keys, and the technical components used to prepare the certificates and time stamps and to ensure that certificates can be checked at any time."

The task to establish in further detail all the technical requirements for digital signatures was assigned to the "Bundesamt fur Sicherheit in der Informationstechnik" (BSI).[57] This administration drafted a series of very detailed documents[58] of which only very simplified and abbreviated versions have been published in the form of official documents. This was, for instance, the case for the requirements for technical components.[59] As far as the technical components for time-stamps are concerned, this document specifies (§ 6: Issue of time stamps):

"The technical components with which time stamps pursuant to § 9 of the Act are generated must function in such a manner that:

[56] § 5(5): "(5) The certification authority shall engage reliable staff for the exercise of certification activities. For the provision of signature keys and the issue of certificates it shall use technical components as set out in §14."

[57] <http://www.bsi.bund.de/esig/index.htm>

[58] <http://www.bsi.bund.de/esig/basics/techbas/masskat/index.htm>

[59] Publication under § 16(6) of the Digital Signature Ordinance of suitable security measures for technical components Security Measures for Technical Components under the Digital Signature Act, 15 July 1998, published in Federal Gazette No 204a of 30 October 1998,
<http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/16.pdf>

- the valid official time, without any distortion, is added to the time stamp when it is generated, and
- security-relevant changes in technical components are apparent for the user (cf. § 16(5) of the Ordinance).

MC 6.1 Use of the official time as given by the Federal Institute of Physics and Metrology for the time stamp service.

MC 6.2 Security measures ensuring that:

- · the actual official time is indicated in the time stamp to be affixed to the data, and
- · the data is digitally signed in their entirety without modification at the stated time.

MC 6.3 Use of technical components for digital key generation which meet the requirements in sections 1 to 3.

MC 6.4 Security measures as in MC 1.4.[60]

MC 6.5 Adequate performance level to minimise the risk of undue delays in the time stamp service."

3.2.3. The 1997 legislation in Italy

The Law nr.59 of 15 March 1997 (the so-called Bassanini law) introduced in Italy the use of electronic documents for legal transactions. The law was completed by the decree nr.513 of 10 November 1997 setting the criteria and methods to be used and a decree of 8 February 1999 on the technical rules laying down the specific technical requirements for electronic documents.[61]

The Italian law of 1997 was very similar to the first German Digital Signature Act It established basically a licensing scheme for certification authorities. Time stamping was considered as one of the activities of such an authority. The Decree of 8 February 1999 contained in Title III detailed technical requirements for time stamping.

[60] MC 1.4 Security measures alerting the user (e.g. by means of external damage or functional disruption) to security-relevant changes (i.e. changes impairing the prescribed security level). If a security-relevant change is not obvious at first sight, it must be ascertainable at least by indirect means (e.g. test procedures).

[61] All these documents can be consulted (in Italian) on the website of the CNIPA: <http://www.cnipa.gov.it/site/it-IT/Le_Attivit%c3%a0/Elenco_certificatori/Normativa/>

3.3. Time-stamping in the European e-Signatures Directive

The enactment of electronic signatures laws in Germany and Italy was the signal for the European Commission to take an initiative in this domain. As usual the European Commission started the preparation of such an initiative with a Communication to the Council of Ministers.

In the Communication "Towards a European framework for digital signatures and encryption" of 1997 the Commission stated:

"There are many situations in legal relations, where proof of the exact time of a certain action (transmission, creation or receipt of a document or the time at which a declaration of intent is made) is crucial. It is important to prove the exact time when a key was revoked to avoid liability for contracts signed with a compromised key. Therefore, digital time-stamping services able to reliably confirm the exact time of certain actions will be necessary. Time stamping services are also crucial for 'Intellectual Property Right' applications. These services could be provided by a CA, but of course also by another body."

In its Communication presenting the first draft of the Electronic Signature Directive the European Commission decides however to focus more or less exclusively on the regulation of certification authorities in the strict sense (issuers of digital signature certificates to the public).

"A certification service provider may offer a wide range of services. The present Directive focuses particularly on certification services in connection with electronic signatures. Certificates can be used for a variety of functions and can contain different pieces of information. The information can include conventional identifiers such as name, address, registration number or social security number, VAT or tax identification number, or specific attributes of the signatory for instance, their authority to act on behalf of a company, their credit worthiness, the existence of payment guarantees, or the holding of specific permits or licenses. As a consequence, a variety of certificates are envisaged for a range of uses. *However, a legal framework is mainly needed for certificates to enable the authentication of the electronic signature of a signing individual. The present Directive therefore focuses on the function of a certificate (called "qualified certificate") as a linkage to the civil identity or the role of a person.* "

In the text of the European Electronic Signatures Directive as it has finally been adopted[62] time-stamping services are considered as a subcategory of certification services. Recital 9 of the European Electronic Signatures Directive states that the definition of "certification services should not be limited to the issuance and management of certificates, but should also encompass any other service using, or ancillary to, electronic signatures, such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures. Article 2(11) of the Directive defines consequently a "certification-service-provider" as "an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures".

Time stamping service providers are therefore submitted to the same legal rules as all other certification service providers. However, it has to be taken into account that most of the provisions of the Electronic Signatures Directive are only applicable to service providers issuing so-called "qualified" certificates to the public. The reason for this is that one of the main provisions of the Directive (Art. 5.1) introduces the principle that advanced electronic signatures based on qualified certificates and created with a secure device, should be considered in all Member States as an equivalent to handwritten signatures.

Qualified certificates are certificates meeting the requirements laid down in Annex I of the Directive and issued by a certification service provider who fulfills the requirements of Annex II.

Annex I lists ten requirements for qualified certificates. They must contain:

- an indication that the certificate is issued as a qualified certificate;
- the identification of the certification service provider and the State in which it is established;
- the name of the signatory or a pseudonym, which shall be identified as such;
- provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

[62] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures, Official Journal of the European Communities L13/12 of 19/01/2000

- signature-verification data which correspond to signature-creation data under the control of the signatory;
- an indication of the beginning and end of the period of validity of the certificate;
- the identity code of the certificate;
- the advanced electronic signature of the certification service provider issuing it;
- limitations on the scope of use of the certificate, if applicable; and
- limits on the value of transactions for which the certificate can be used, if applicable.

The ETSI Technical Specification (TS 101 862) defines how the X.509 public key certificate format may be used to meet the requirements of Annex I of the Directive. In addition, where there is currently no defined mechanism for meeting a requirement (e.g. limits on the value of the transaction) the specification builds on the existing extension capabilities of X.509 to define the necessary optional data structures.[63]

The European Directive doesn't mention anything such as "qualified time-stamps". The concept of "qualified certificate" is clearly restricted to identity certificates, establishing the link between a public key and a duly identified person.

Certification service providers issuing "qualified certificates" must, following Annex II:

- demonstrate the reliability necessary for providing certification services;
- ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
- ensure that the date and time when a certificate is issued or revoked can be determined precisely;
- verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;
- employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in

[63] ETSI TS 101 862 V.1.2.1 (2001-06) is available at <http://webapp.etsi.org/exchangefolder/ts_101862v010201p.pdf>

particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;

- use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;[64]
- take measures against forgery of certificates, and, in cases where the certification service provider generates signature-creation data, guarantee confidentiality during the process of generating such data;
- maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;
- record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;
- not store or copy signature-creation data of the person to whom the certification service provider provided key management services;
- before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable

[64] The security requirements for trustworthy systems managing certificates for electronic signatures have been specified in two related CEN Workshop Agreements (CWAs). The first, CWA 14167 Part 1, specifies overall security requirements on trustworthy system components, used by Certification Service Providers (certification service providers), to create standard qualified certificates. The second, CWA 14167 Part 2, defines specific requirements on the CSP's cryptographic modules. By conforming to these specifications, a CSP's systems and its cryptographic devices fulfil the requirements for trustworthy systems stated in point f) of the Annex II of the Directive. The Workshop Agreements relating to electronic signatures are available at <http://www.cenorm.be/cenorm/businessdomains/businessdomains/informationsocietystandardizationsystem/published+cwas/cwa+download+area.asp>

language. Relevant parts of this information must also be made available on request to third parties relying on the certificate;

(l) use trustworthy systems to store certificates in a verifiable form so that:

- only authorised persons can make entries and changes,
- information can be checked for authenticity,
- certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
- any technical changes compromising these security requirements are apparent to the operator.

The requirements of Annex II of the Directive are only applicable to certification service providers issuing qualified certificates to the public. It has certainly never been the intention of the European legislator to apply these requirements to “qualified” time-stamp providers.

The foregoing conclusion doesn't mean that the European Electronic Signature Directive is completely irrelevant for time service providers.

The central provision concerning certification services – in its widest sense – is Article 4.1 of the Directive. It provides that each Member State shall apply the national provisions, which it adopts pursuant to the Directive, to certification service providers established on its territory and to the services they provide. Member States may not restrict the provision of certification services originating in another Member State in the fields covered by this Directive.

Article 4 introduces, in other words, the “country of origin” principle for certification services. Certification service providers – including trusted time service providers - are submitted to rules of the country in which they are established (their “country of origin”). They do not have to take into account the rules of all the European countries in which they provide their services. Once they respect the rules of the country in which they are established, their services have to be considered in line with the rules of all the Member States in which they operate. In every Member State, providers originating in other Member States should have the same chances for providing their services as the providers established in the Member State, particularly in the fields covered by the Directive. Especially supervision or accreditation schemes should never lead to legal or practical restrictions for the provision of certification services by providers established in other Member States.

Another provision of the European Electronic Signature Directive that can be applied without any difficulty to time-stamping providers, is Art. 3.2 which deals with voluntary accreditation. Article 3.2 states that, without prejudice to the prohibition formulated in Article 3.1 (prohibition for Member States to submit certification services to prior authorisation) , "Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification service provision". Article 2.13 defines voluntary accreditation as "any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification service provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification service provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body".

Further, according to Article 3.2 of the Directive, "all conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification service providers for reasons which fall within the scope of this Directive." Recital (11) explains that "voluntary accreditation schemes aiming at an enhanced level of service-provision may offer certification service providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market; such schemes should encourage the development of best practice among certification service providers; Certification service providers should be left free to adhere to and benefit from such accreditation schemes". In Recital (12) it is stated that "Member States should not prohibit certification service providers from operating outside voluntary accreditation schemes" and that "it should be ensured that such accreditation schemes do not reduce competition for certification services".

The idea behind a voluntary accreditation scheme is that it offers an incentive for service providers to offer high quality services to meet the requirements of the accreditation scheme. The certified proof of compliance will help to attract potential clients. Voluntary accreditation schemes are supposed to have the advantage of being able to adapt more easily to developments in a quickly changing technical environment. Since accreditation schemes are regulated by market forces - i.e. the market players have to gauge if the expected rise in revenue generated by the anticipated increase of consumer trust is worth the necessary investment for complying with the security requirements of an accreditation scheme - they are assumed to be able to adapt to business needs more quickly.

The European legislator has estimated, very rightly, that voluntary accreditation schemes could be beneficial for the development of the market. It can give certification service providers operating in Europe the possibility of demonstrating their level of security and trustworthiness. Accreditation schemes could certify the adequacy of the security level of a particular certification service for use in particular contexts or applications. For instance, specialized accreditation schemes could certify the quality of trusted time service providers.

Recital (11) of the Directive also refers to the evolving market in this area. When new solutions are discovered and introduced into the market, accreditation schemes can help providers gain user trust. The accreditation schemes should mainly be created or maintained for the benefit of the providers themselves. They should encourage the development of best practices and remain up-to-date with state-of-the-art technology in the sector. They are a form of common quality control, organized at the level of a particular sector. The Directive encourages the creation of such schemes, as long as the conditions related to those schemes are objective, transparent, proportionate and non-discriminatory.

To conclude this paragraph about the relevance of the European Electronic Signatures Directive for companies offering time services in Europe, it appears from the preceding considerations that the following rules are important in this context:

1. It is strictly prohibited for EU Member States to submit the provision of trusted time services to any form of prior authorisation, for example in the form of a licensing scheme.

2. A time service provider established in the EU has to respect the legal rules of the Member State where he is established (rule of

origin). It is not necessary to be compliant with the legal provisions of every Member State on which territory time services are provided.

3. Voluntary accreditation schemes for time services can be established or maintained under the condition that they are based on objective, transparent, proportionate and non-discriminatory criteria. It is important to stress that the accreditation schemes have to remain voluntary.

3.4. Time-stamping standardization

Important standardization efforts have been undertaken in the area of time-stamping services, at the European level – in the context of the EESSI – as well as at the international (ISO) and the global (Internet IETF) level.

3.4.1. The European Electronic Signature Standardization Initiative

In 1998, parallel to the preparation of the Electronic Signatures Directive the European Commission has given a mandate to the European standardization organizations to start standardization activities in the area of electronic signatures. This mandate has led to the establishment of the "European Electronic Signatures Initiative (EESSI).[65] The standardization initiative started with the drafting of a work plan, which was submitted and later also approved by the European Commission.

The proposed EESSI work plan contained the following considerations about time-stamping services:

- Nearly all the requirements for security management of a time-stamping service can be addressed through adoption of a general security management standard such as BS 7799. The only potential area of concern specific to time-stamping is clock precision.

- As for certification service providers issuing qualified certificates the use of trustworthy system and products is necessary. It is suggested that the same requirements apply for use of trusted

[65] <http://www.ictsb.org/EESSI_home.htm>

systems and products by certification service providers issuing trusted time-stamps.

- An Internet draft is under development which may be used as the basis for a technical profile.
- As with certification service providers issuing qualified certificates, certification service providers issuing trusted time-stamps should operate within a defined policy, which may be published as a practice statement.
- In order to re-verify the validity of a signed document years later after it has been signed, it is important to reliably know that it was signed during the validity period of the certificates. The appropriate use of time stamps delivered by one or more time stamping authorities is able to address these issues. A protocol to interoperate with time stamping authorities is needed. Such a protocol is being defined within the IETF by the PKIX working group.

On the basis of these considerations, the EESSI defined a standardizatin work area relating to "security management and policy for certification service providers issuing trusted time-stamps". For this work area the following standardization tasks were proposed:

- Security management requirements for certification service providers issuing trusted time-stamps.
- Requirement for use of trusted systems and products by certification service providers issuing trusted time-stamps.
- Technical profile for certification service providers issuing trusted time-stamps.
- Standardized policy for certification service providers issuing trusted Time-stamps
- Agreement on conformance assessment requirements for certification service providers issuing trusted time-stamps.

Up to now the work plan resulted in two deliverables, published as ETSI technical specifications:[66]

- ETSI TS 101 861: the purpose of this standard is to specify format and protocol for time stamping. The standard is a profile of RFC 3161 "Time Stamp Protocol". TS 101 861 Version 1.2.1 was published in March 2002.

[66] See further: <http://portal.etsi.org/esi/el-sign.asp>

- ETSI TS 102 023: this standard specifies policy requirements relating to the operation of Time-stamping Authorities (TSAs). It defines policy requirements on the operation and management practices of TSAs such that subscribers and relying parties may have confidence in the operation of the time-stamping services.
  The policy requirements are primarily aimed at time-stamping services used in support of qualified electronic signatures (i.e. in line with article 5.1 of the European Directive on a community framework for electronic signatures) but may be applied to any application requiring to prove that a datum existed before a particular time. They are based upon the use of public key cryptography, public key certificates and reliable time sources. The first version of this document was published in April 2002.

A third standardization document – ETSI TS 101 733: Electronic Signature Formats - allthough not focusing specifically on time-stamping, has to be mentioned in this context because it describes a format for electronic signatures relying heavily on the use of time stamps. The original version of May 2000 required the use of time stamps for long term validation of electronic signatures. The current version – ETSI TS 101 733 v 1.2.2 - is an amended version that no longer mandates the use of time stamps. For long term validation secure record archiving is accepted as an alternative to time stamps.

A fourth standardization document – ETSI TS 101 903 - defines XML formats for advanced electronic signatures that remain valid over long periods of time, are compliant withe the European Directive and incorporate additional useful information in common use cases. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the signature. The standard – commonly called "XADES" - uses a signature policy, implicitly or explicitly referenced by the signer, as the basis for establishing the validity of an electronic signature. It uses time-stamps or trusted records (e.g. time-marks) to prove the validity of a signature long after the normal lifetime of critical elements of an electronic signature and to support non-repudiation. It also specifies the optional use of additional time-stamps to provide very long-term protection against key compromise or weakened algorithms.

The standard also specifies the use of the corresponding trusted service providers (e.g. time-stamping authorities), and the data that needs to be archived (e.g. cross certificates and revocation lists). An advanced electronic signature aligned with the XADES specification can, in consequence, be used for arbitration in case of a dispute between the signer and verifier, which may occur at some later time, even years later. The document builds on the standards for Electronic

Signatures defined in *IETF W3C: XML-Signature Syntax and Processing*[67] and *ETSI TS 101 733: Electronic Signature Formats*.

3.4.2. ISO draft standards for time stamping services

Important standardization efforts with regard to time-stamping services have also been undertaken in the context of the ISO. Under the general title "Information technology - Security techniques - Time-stamping services" a three part document has been drafted:

- Part 1: Framework
- Part 2: Mechanisms producing independent tokens
- Part 3: Mechanisms producing linked tokens

1. ISO/IEC 18014-1: Part 1 ("Framework") 1. identifies the objective of a time-stamping authority; 2. describes a general model on which time- stamping services are based; 3. defines time-stamping services; 4. defines the basic protocols of time-stamping; 5. specifies the protocols between the involved entities.
2. ISO/IEC 18014-2: Part 2 ("Mechanisms producing independent tokens") defines time-stamping mechanisms that produce independent tokens, which can be verified one by one. A time-stamping service provides evidence that a data item existed before a certain point in time. Time-stamp services produce time-stamp tokens, which are data structures containing a verifiable cryptographic binding between a data item's representation and a time-value.
3. ISO/IEC 18014-3: Part 3 ("Mechanisms producing linked tokens") describes a general model for time-stamping services producing linked tokens and describes the basic components used to construct a time-stamping service of this type. It defines the data structures used to interact with a time-stamping service of this type and describes specific instances of such time-stamping services.

3.4.3. Standardization in the context of the IETF

As far as the Internet Engineering Task Force (IETF) is concerned,

[67] <http://www.w3.org/TR/2000/CR-xmldsig-core-20001031/>

standardization relevant for time-stamping services has mainly been undertaken in the PKIX (public key infrastructure) and, more recently, in the LTANS (long-term archive and notary services) work groups. These efforts have thus far resulted in the following documents:

RFC3161 – Internet X.509 PKI Time-Stamp Protocol (TSP)[68]: this document describes the format of a request sent to a Time Stamping Authority (TSA) and of the response that is returned. It also establishes several security-relevant requirements for TSA operation, with regards to processing requests to generate responses.

RFC3628 - Policy Requirements for Time-Stamping Authorities (TSA): this document defines requirements for a baseline time-stamp policy for Time-Stamping Authorities (TSAs) issuing time-stamp tokens, supported by public key certificates, with an accuracy of one second or better. A TSA may define its own policy which enhances the policy defined in RFC3628. Such a policy shall incorporate or further constrain the requirements identified in this document.

Besides the preceding standardization documents, a few interesting Internet Drafts with relevance for time-stamping services have also been presented in the area of long-term archiving and notary services.[69]

3.5. National regulatory frameworks for time-stamping services in the EU

The use of time stamps is explicitly mentioned in the electronic signature legislation of Austria, Germany and Italy. All these legislations contain a legal definition of time stamps. A time stamp is mostly defined as a certificate issued and signed by a certification service provider in which this provider certifies that certain data have been submitted to him at a certain point in time. It is mainly used as a means of evidence to proof that these data existed before the moment of time-stamping and that they haven't been altered since then.

[68] <http://www.ietf.org/rfc/rfc3161.txt>

[69] <http://www.ietf.org/internet-drafts/draft-ietf-ltans-reqs-00.txt>

In many countries time-stamping providers have the possibility to submit their services to a voluntary accreditation scheme. Such possibilities exist, for instance, in Austria, Germany, Luxembourg and in the U.K. For the time being, it is not yet possible to get time-stamping services accredited in Belgium.

Because, compared to other EU Member States, Germany has very detailed rules in this area, the following pages make a distinction between the regulatory framework for Germany and the one for "other European countries".

3.5.1. Germany

The German law, revised in 2001 in order to make it compliant with the European Directive, contains a paragraph on "qualified time-stamping providers".[70] Qualified time-stamping providers are defined as time-stamping providers who fulfill a series of security requirements that are very similar to the requirements of Annex II of the European Electronic Signature Directive.

A provider who claims to be a "qualified time-stamping provider" has to notify this first to the public authorities (REGTP). Following the Ordinance of 22 November 2001[71]

(1) A notification pursuant to Section 4 (3) of the Signatures Act shall be submitted to the competent authority in written form or furnished with a qualified electronic signature pursuant to the Signatures Act.

(2) The notification must contain the following details and documentation:

1. the name and address of the certification service provider,
2. the names of the legal representatives,
3. current certificates of good conduct pursuant to Section 30 (5) of the Federal Central Register Act for the certification service provider and his legal representatives,
4. a current extract from the commercial register or a comparable

[70] <http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/119.pdf> The Signatures Act (Framework for Electronic Signatures, Amendment of Further Provisions Act of 16 May 2001, Federal Law Gazette I, p 876) was published on 21 May 2001 and has been in force since 22 May 2001

[71] <http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/120.pdf>

document,

5. documents to prove the necessary technical, administrative and legal specialised knowledge pursuant to Section 4 (2) sentence 3 of the Signatures Act,

6. a security concept with a precise explanation of how this is implemented, including the delegation of functions to third parties pursuant to Section 4 (5) of the Signatures Act, and

7. proof of financial cover pursuant to Section 12 of the Signatures Act.

The security concept pursuant to Section 4 (2) sentence 4 of the Signatures Act has to contain the following:

1. a description of all necessary technical, structural and organisational security measures and their appropriateness,

2. a list of the products used for qualified electronic signatures with manufacturer declarations pursuant to Section 17 (4) sentence 2 or certifications pursuant to Section 17 (4) sentence 1 or Section 15 (7) sentence 1 of the Signatures Act,

3. an overview of the organisation of the establishment and operations and of the certification activities,

4. the precautions and measures to secure and maintain operations, especially in case of emergencies,

5. the procedures to assess and secure the reliability of the personnel, and

6. an assessment and evaluation of the remaining security risks.

The documentation pursuant to Section 10 of the Signatures Act must comprise the security concept, including any amendments, the documents regarding the specialised knowledge of the persons working in the company and the contractual arrangements with the applicants.

Section 9 of the Ordinance contains the details of the financial aspects:

1. The financial provision pursuant to Section 12 of the Signatures Act can be supplied 1. by a liability insurance policy with an insurance company authorised to operate in the area covered by this Act or 2. by an indemnification or guarantee commitment by a bank authorised to operate in the area covered by this Act if it

ensured that it offers security comparable to a liability insurance policy. (

2. Where the provision is supplied by means of an insurance policy pursuant to subsection (1) no. 1, the following provisions apply: 1. Section 158b (2) and Sections 158c to 158k of the Insurance Contract Act shall apply to this insurance policy. The competent authority pursuant to Section 158c (2) of the Insurance Contract Act shall be the authority pursuant to Section 66 of the Telecommunications Act. 2. The minimum sum insured must be 2.5 million euro for each insured event. An insured event shall be each occurrence causing liability related to the individual event pursuant to Section 12 (1) of the Signatures Act, irrespective of the number of resulting cases of damage. Any arrangement according to which an error which affects several certificates, time stamps or the information pursuant to Section 5 (1) sentence 2 of the Signatures Act is regarded as one insured event shall not be permissible. If a maximum annual amount for all damages caused in one year of cover is agreed upon, this amount shall total at least four times the minimum sum insured.

If the preceding procedure has been followed, the time-stamping provider is considered as a provider who issues “qualified” time stamps. This can have some legal consequences inside Germany. Section 17 of the Ordinance regulates the period and procedure for long-term data security. Pursuant to Section 6 (1) sentence 2 of the Signatures Act, data with a qualified electronic signature shall be re-signed if they are required in signed form for a period longer than that for which the algorithms and related parameters used to create and verify them are considered to be suitable. In this case the data shall be furnished with a new qualified electronic signature prior to the time at which the suitability of the algorithms and related parameters ends. This signature has to be furnished with suitable new algorithms or related parameters, include earlier signatures and bear a *qualified time stamp*.

In order to become a “qualified” time-stamp provider in Germany, it is not necessary to obtain any form of accreditation. It is sufficient to fulfill the notification requirements as described above. However, if they wish so, time-stamp providers can get accredited by submitting their services to a voluntary accreditation scheme. Essentially the voluntary accreditation scheme controls the conformity of the “security concept” (see above) of the applicant with the legal requirements for “qualified” certification service providers. For time-stamping providers this means that the entity performing this control will also take a look at the specific technical environment for time-stamping, as far as this environment has been included in the security concept of the applicant.

The list of accredited certification service providers and of the recognized evaluation and certification bodies is published on the website of REGTP.[72]

3.5.2. Other European countries

Although the regulatory framework is far from being as explicit and detailed as the one in Germany, time-stamping service providers can also get accredited in other European Member States. Such possibility exists, for example, in Austria, Luxembourg or in the UK.

In later versions of this paper we will provide more details about the accreditation schemes in these countries.

3.5.3. Belgium[73]

The Belgian legislation with regard to electronic signatures doesn't explicitly mention time stamping or trusted time services. However, since this legislation is an almost literal copy of the European e-Signatures Directive, time-stamping service providers are considered as a subcategory of certification service providers.[74]

Similar to what is possible in Germany, a time-stamping provider can be recognized as a qualified certification service provider under the condition that he fulfills the requirements of Annex II of the European Directive – these requirements have been literally transcribed in Annex II of the Belgian law – and provided that the issued time stamps take the form of a qualified certificate or, in other words, have a format that is fully compliant with Annex I of the Directive (copied as Annex 1 in the Belgian law).

To become officially recognized as a qualified certification provider in Belgium it is necessary to send a notification to the Federal Public Service (FPS) "Economy, SMEs, Self-employed and Energy" (the

[72] <http://www.regtp.de/en/tech_reg_tele/start/in_06-02-02-00-00_m/index.html>

[73] The information about the legal situation in Belgium represents the personal view of the authors of this paper and has not yet been checked with the representatives of the competent administration.

[74] Art. 2, 10° of the Law of 9 July 2001 establishing certain rules with regard to the legal framework for electronic signatures and certification services,

former Federal Ministry of Economy).[75] The information to be provided with this notification is limited to: name, address and contact data (incl. e-mail address) and the usual identification data (company register) of the provider, plus an attestation that an insurance policy has been subscribed for the coverage of the professional liability of the provider. Within five days after this notification the public administration has to send a receipt and includes the data of the provider in the register of qualified certification service providers established in Belgium.[76]

Article 17 of the Belgian law of 9 July 2001 determines that a qualified certification service provider issuing qualified certificates and using secure signature-creation devices (compliant with Annex III of the EU Directive), can apply for an accreditation. The application has to be transmitted to the Administration for Electronic Signatures of the FPS Economy. The details of the accreditation procedure leading to the BE.SIGN accreditation are contained in the Royal Decree of 6 December 2002 relating to the organisation of the control and the accreditation of certification service providers issuing qualified certificates.[77]

[75] FPS Economy, Administration Electronic Signatures, Mr. Jean-François Petit, WTC III, Boulevard Simon Bolivar 30, B-1000 Brussels, Tel. 208 36 42, e-mail: be.sign@mineco.fgov.be

[76] The register can be downloaded from <http://www.mineco.fgov.be/information_society/e-signatures/ list_e_signature_fr.pdf>

[77] <See http://www.mineco.fgov.be/information_society/e-signatures/ law_e_signature_004.pdf>

4. Concluding remarks

In this research paper several interesting points have surfaced:

- An internationally recognized time-scale is a necessity in civil society. UTC, the time-scale provided by the BIPM, currently fulfills this function and is legally recognized in several countries.
- Time-stamps are valuable tools in the legal context for various reasons. Firstly, a time-stamp from a trustworthy time-stamping authority adds a reliable time indication to electronic records, proving that the file existed at a certain point in time. Secondly, a time-stamp functions as a seal that can guarantee the integrity of a record.
- The regulatory framework applicable to time services is minimal, thus leaving the market free range. The framework on electronic signatures is applicable to time-stamping in principle, but in effect mainly regulates certificate creation and management. Allthough the regulatory framework focuses on identity certification service providers, it is flexible enough to encompass time certification services as well and voluntary accreditation as a time-stamp certification service provider is currently possible in some countries of the EU.