Authenticity and Authentication Issues in the Italian and European Union Legislation

Compiled by Fiorella Foscarini

September 2005

CIVIL CODE

Book I, Title XIV (About Registry Office Records)

Art. 451 (Probative value of the acts issued by the Registry Office)
Records issued by the Registry Office fully prove what the public officer attests to be happened in front of him/her or to be done by him/her, until anybody actions for forgery *[querela di falso]*. Witnesses' declarations make proof to the contrary.

Art. 452 (Absence, destruction, or loss of registers)
In case either the registers have not been kept or have been destroyed or lost, or, for any other reason, the registration of the act is completely or partially missing, birth or death proof can be given by any means.
In case of absence, partial or total destruction, manipulation or concealment due to the requester's fraudulent intention, the latter is not admitted to the proof as above.

Art. 453 (Annotations)
No annotation can be made on any record that has already been registered, unless such annotation had been provided by law or ordered by the judicial authority.

Art. 454 (Amendments)
Amendments on civil status records must be ordered via final judgement of the court to the public officer. The latter can be ordered either to correct an existing record or to enter an omitted one in the register, or to remake a record which has been lost or destroyed. Such final judgements must be recorded in the registers.

Book VI, Title I (About Recording)

Art. 2658 (Land Registry records)
The party who wants to register a contract must provide the Land Registry officer with either a certified copy, in case of public records or sentences, or the original, in case of private deeds, unless the latter has been deposited in a public archives or at a notary. In this case, a true copy signed by either the archivist or the notary is enough.

Art. 2673 (Land Registry officer's obligations)
The Land Registry officer must issue copies of the registration entries and annotations – or a certificate which states that there is no registration or annotation – to anybody asking for them. (…) He or she also must issue copies of the original records that have been

deposited at the Land Registry or of those records whose originals have been deposited at a notary or in a public archives, both located outside the jurisdiction of the Land Registry.

Art. 2676 (Differences among registers, copies and certificates)
In case of differences among the register entries and what is stated in the copies or in the certificates issued by the Land Registry officer, the content of the registers prevails.

Book VI, Title II (About Evidence)

Art. 2699 (Public record)
Public record refers to the record that has been written, according to required formal elements, by a notary or any other public officer who is authorized to confer public trustworthiness to a record in the place where it was created.

Art. 2700 (Probative value of public records)
A public record fully proves the provenance of a record from the public officer that has created it, and is evidence of parties' declarations and any other facts which the public officer attests to be happened in front of him/her or to be done by him/her, until anybody actions for forgery.

Art. 2701 (Public record conversion)
A record which has been created by an incompetent or unable public officer, or which is not compliant with the required formal elements, if it has been signed by the parties, has the same probative value as that of a private deed.

Art. 2702 (Probative value of private deeds)
A private deed fully proves the provenance of the declarations from the person who has signed it, if the signature either is recognized by whom the deed has been made against or is legally ascertained, until anybody actions for forgery.

Art. 2703 (Signature authentication)
The law recognizes the signature that has been authenticated by a notary or any other authorized public officer. Authentication involves the public officer attesting that the signature has been affixed in front of him/her. The public officer must ascertain the identity of the signatory beforehand.

Art. 2712 (Mechanical copies)
Photographic or cinematographic copies, phonographic recordings and in general any other mechanic representations of facts and things, fully prove the facts and things they document, if the person against whom those copies are introduced does not deny that they correspond to those facts and things.

Art. 2714 (Copies of public records)
Copies of public records that are sent from authorized public depositories according to the prescribed forms have the same probative value as that of the original. The same

probative value is also recognized to the copies of the copies of original public records that are sent from authorized public depositories.

Art. 2715 (Copies of original deposited private deeds)
Copies of private deeds which are deposited in public offices and are sent from authorized public depositories have the same probative value as that of the original record they are made from.

Art. 2716 (Absence of the original record or a deposited copy)
In case of absence of the original public record or a copy of it in a public depository, the copies that have been sent according to art. 2714 have full probative value. However, if such copies, as well as an existing copy of a missing original which is kept by a public depository, show deletions, erasures, insertions or any other external defects, it is up to the judge to weigh their probative value. The same principle applies to private deeds.

Art. 2717 (Probative value of other copies)
Copies made by public officers outside the above mentioned cases have the value of written presumptive evidence.

Art. 2718 (Probative value of incomplete copies)
Incomplete copies or abstracts which are made according to the prescribed form by authorized public officers, who are the depositories of the originals, have full probative value only with regard to the portion of the original they literally reproduce.

Art. 2719 (Photocopies)
Photocopies of records or deeds have the same probative value as that of true copies, if the fact that they are compliant with the original is attested by a competent public officer or it is not explicitly unrecognized.

Art. 2720 (Probative value)
Ascertainment or renovation records fully prove the content of the original record, if one does not demonstrate, by showing the latter, that a mistake was made in the ascertainment or renovation.

Art. 2214 (Mandatory account books and other documentation)
Any entrepreneur is obliged to keep account books and inventories. He also has to keep any other account documentation and, in an orderly way for each business transaction, preserve the originals of every received letter, telegram and invoice, as well as the copies of every sent letter, telegram and invoice. All this does not apply to minor entrepreneurs.

Art. 2721 (Admissibility: value limits)
Testimonial evidence with regard to contracts is not admissible when the object's value exceeds L. 5.000 (i.e., Euro 2.5). However, the judicial authority may allow testimonial evidence below the above-mentioned limit taking into consideration the parties' quality, the nature of the contract and any other circumstance.

Art. 2722 (Added or opposite agreements)
Testimonial evidence is not admissible when it refers to agreements which have been added to or are against the content of a record, and which have been stipulated beforehand or contemporaneously.

Art. 2723 (Subsequent agreements)
If an added or opposite agreement that was stipulated after the creation of a record is introduced, the judicial authority can admit testimonial evidence only if, after considering the parties' quality, the nature of the contract and any other circumstance, it looks likely that additions or changes to the record have been made.

Art. 2724 (Exceptions to testimonial evidence non-admissibility)
Testimonial evidence is always admissible when:
1. a written evidence basis exists: that is any written document made by the inquired person which supports the facts;
2. the contracting party could not morally or physically get a written evidence;
3. the contracting party has guiltlessly lost the record that was his/her evidence.

Art. 2725 (Mandatory written evidence)
When, according to the law or the parties' will, a contract must be proved in writing, testimonial evidence is only allowed under no. 3 of the above-mentioned article. The same rule applies when the written form is necessary to not incur the nullity of a deed.

Art. 2728 (Evidence against presumptions of law)
Presumptions of law exempt from any evidence those in whose favour they are established. Evidence to the contrary cannot be given against those presumptions on which basis the law declares invalid certain documents or when lawsuit is not admissible.

Art. 2729 (Simple presumptions)
Presumptions which are not established by the law are left to the judge's prudence. The judge can only admit serious, detailed and consistent presumptions. In such cases when the law does not admit testimonial evidence, presumptions cannot be admitted as well.

L 59/1997[1], art. 15

Documents, records, and data created by public and private entities by means of computerized or telecom-tools, as well as contracts drawn up in the same way, and their filing and transmission via electronic devices, are valid and effective for all legal purposes. Criteria and methods on how to enforce this article will be defined in specific regulations to be issued.

DPR 445/2000[2], art. 6

[1] Legge n. 59 del 15 marzo 1997: "Delega al Governo per il conferimento di funzioni e compiti alle Regioni ed Enti Locali, per la riforma della PA e per la semplificazione amministrativa".

Records reproduction and preservation:

1. Public administrations and private entities are allowed, for all legal purposes, to replace the original documents in their archives, as well as all accounting records, correspondence, and any other kinds of deed that are meant to be preserved according to the law, with their copy on any photographic or digital medium which is suitable for producing true copies.

2. Preservation obligations are fully satisfied, both for administrative and probative purposes, also with the use of digital media when the employed procedures comply with the technical rules provided by the Authority for Information Technology in the Public Administration (AIPA).

DPR 445/2000, art. 8
Electronic records:

1. Electronic records that are created by anybody, as well as their registration on digital media, and transmission via telecom-tools, are valid and effective for all legal purposes when complying whit this regulation.

2. Technical rules for creation, transmission, preservation, duplication, copy, and validation of electronic records are established by Prime Minister's Decree, in accord with AIPA and the Guarantor for the protection of sensitive data. In order to be abreast of technological progress, those technical rules should be updated every second year at least.

DPR 445/2000, art. 9
Public administrations' electronic records:

1. Any data or document electronically created by any public administration represents a primary and original source of information that may be used to make copies on any kind of medium for all legal purposes.

2. In all operations relevant to creation, transmission, preservation, and reproduction of data and documents by using computerized systems, *[meta-]*data about both the concerned administrations and the authors of such operations must be easily identifiable.

DPR 445/2000, art. 10
Form and effectiveness of electronic records:

1. Any electronic record which has been signed by means of digital signature and which has been drawn up according to the established technical rules is compliant with the

[2] Decreto del Presidente della Repubblica n. 445 del 28 dicembre 2000: "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa".

legal requirement of the written form and has probative value according to art. 2712 of the Civil Code. ➔ Replaced, according to **Dlgs 10/2002**[3], art. 6, by the following art. 10:

1. An electronic record has probative value according to art. 2712 of the Civil Code with regard to the facts and things it documents.
2. An electronic record which has been signed by means of electronic signature meets the legal requirement of the written form. As regards its probative value, the record itself is freely assessable, taking its objective quality and security features under consideration. It also fulfils all obligations as laid down in art. 2214 of the Civil Code, as well as any other similar legislative or regulatory disposition.
3. An electronic record, when it has been signed by means of digital signature or any other kind of advanced electronic signature, and the signature is based on a qualified certificate and has been created by means of a secure-signature-creation device, represents full evidence of the provenance of its content from the person who signed it, until anybody brings an action of false *[querela di falso]*.
4. An electronic record which has been signed by means of electronic signature cannot, however, be rejected as legally irrelevant, nor its admissibility as evidence can be denied just because it has been electronically signed, or because its signature is not based on a qualified certificate, or because the signature has not been created by means of a secure-signature-creation device.

DPR 445/2000, art. 11, as amended by DPR 137/2003[4], art 4
Electronically stipulated contracts:

1. Contracts that are stipulated electronically or via telecom-tools and that are signed by means of qualified electronic signature *[replaces "digital signature"]* according to the present rules are valid and effective for all legal purposes.

DPR 445/2000, art. 18
True copies:

1. True copies, either complete or partial, of original records may be made by using any procedure which is able to guarantee an exact and stable *[fedele e duratura]* copy of such records.

2. Copy authentication can be done by the public officer who is responsible for issuing or keeping the original or by the one who is supposed to collect such copy, as well as by a notary, chancellor, municipal secretary or any other officer who has been delegated by the mayor. Authentication involves attesting that such a copy is compliant with the original, by writing so at the very end of the copy. The authorized public officer is also requested to state the date and place of the making of the copy, the number of pages the

[3] Decreto Legislativo n. 10 del 23 gennaio 2002: "Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche".
[4] Decreto del Presidente della Repubblica n. 137 del 7 aprile 2003: "Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislative 23 gennaio 2002, n. 10".

copy consists of, his/her own name, surname and role in the organization, as well as to sign in the margin of each intermediate page. As regards copies of electronic records, see at art. 20.

DPR 445/2000, art. 20
Copies of electronic records:

1. Duplicates, copies and abstracts of electronic records, also those reproduced on different kinds of media, are valid and effective for all legal purposes if they comply with the present provisions.

2 [as amended by DPR 137/2003, art. 6]. Electronic records containing copies or reproductions of public records, private deeds or documents in general, included any kinds of administrative records sent or received by authorized public depositories and public officers, are fully effective according to arts. 2714 and 2715 of the Civil Code, if they are associated with a qualified electronic signature *[replaces "the digital signature of the person responsible for sending or issuing such records"]*.

3. Any electronic copy of records which had originally been created on paper, have the full capacity to replace the original record if such a copy is authenticated by a notary or any other public officer authorized to make certified copies.

5. The obligation of preserving and exhibiting records according to the current enabling legislation is perfectly fulfilled by means of electronic records when the latter are created by following the procedures established in the technical rules.

DPR 445/2000, art. 23
Digital signature:

2. Affixing or associating a digital signature to an electronic record is equivalent to signing a paper record according to the law.
➔ Replaced, according to DPR 137/2003, art. 9, by the following art. 23:
4. Affixing a digital signature supplements and replaces, for any legal purposes, the use of seals, punches, stamps, countermarks and any kinds of marks.

DPR 445/2000, art. 24
Authenticated electronic signature:

1. It is considered as an acknowledged digital signature, according to art. 2703 of the Civil Code, the digital signature whose affixing is authenticated by a notary or any other authorized public officer.

2. Authenticating a digital signature involves a public officer to attest that the digital signature has been affixed in front of him/her by the holder, against previous assessment of the latter's personal identity, of the key validity, and of the fact that the signed

document corresponds to the party's will and is not in conflict with art. 28, par. 1 of L. 89/1913.

DPR 445/2000, art. 25
Signature of public administrations' electronic records:

1. In all electronic records created by public administrations the original hand signature or whatever provided signature is replaced by the digital signature according to the present regulation.

Dlgs 10/2002, art. 2 and **DPR 137/2003, art. 1** [partly replacing DPR 445/2000, art. 1]
Definitions:

- "Digital signature": a special kind of qualified electronic signature that is based on a system of asymmetric keys, of which one public and one private, and that allows both signatory and addressee, through the private and the public key respectively, to make evident as well as verify the provenance and integrity of any electronic record or group of electronic records;
- "Electronic signature": the whole of the data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of computerized authentication;
- "Advanced electronic signature": electronic signature which is the result of a computerized procedure able to guarantee the univocal link to the signatory and his univocal identification, and which is created using means that the signatory can maintain under his sole control, and is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
- "Qualified electronic signature": advanced electronic signature that is based on a qualified certificate and has been created by means of a secure-signature-creation device;
- "Certification-service-providers": entities that issue electronic certificates and provides other services related to electronic signatures;
- "Accredited certification-service-providers": certification-service-providers that have been accredited in Italy or in other Member States;
- "Electronic certificates": electronic attestations which link signature-verification data to the relevant holders and confirm the identity of those holders;
- "Qualified certificates": electronic certificates which meet the requirements laid down in Annex I of the Directive No. 1999/93/CE and are provided by certification-service-providers who fulfil the requirements laid down in Annex II of that EU Directive;
- "Secure-signature-creation device": device which is used to create an electronic signature and meets the requirements laid down in Annex III of the EU Directive.

DPR 137/2003, art. 15 [as added to DPR 445/2000, art. 29]
Certification-service-provider's obligations:

- To publish notice of the annulment or suspension of the electronic certificate upon request of the holder, in case the key has been lost, upon request of the authority, when there are limiting causes of the holder's capacity, in cases of suspicion of abuses or forgery;
- To preserve electronic or manual recording of all information relevant to any qualified certification for ten years, with the purpose to provide evidence of such certification in case of legal proceedings;
- Neither to copy nor to keep any of the private keys that have been provided the holder with;
- To use secure systems for the management of the certification register, in order to guarantee that all entries and changes be exclusively made by the authorized individuals, the authenticity of information be verifiable, certifications be accessible to the public only when that is allowed by the holder, and the operator be in the position to know about any event that might jeopardize the security requirements.

Use of pseudonyms:
Instead of the holder's name, the certification-service-provider can report on the electronic certificate a pseudonym. In case of qualified certification, information relevant to the holder's real identity must be preserved for at least ten years after the expiration of the relevant certification.

Special rules that apply to public administrations:
In order to sign electronic records of external relevance, when signature is required, public administrations are allowed:
a) to directly issue qualified certifications, after having been accredited to do so;
b) to refer to accredited certification-service-providers.
With reference to creating, managing and signing electronic records of solely internal relevance, each administration is allowed to autonomously adopt its own internal rules.

CNIPA's Deliberation 11/2004[5], art. 1
Definitions:

a) "Document": electronic or analog configuration of acts, facts and data which are intelligible directly or through an electronic processing;
b) "Analog document": document created using a physic quantity (magnitude?) that assumes continuous values, such as signs on paper (e.g., paper documents), images on film (e.g., microfiche and microfilm), magnetization on tape (e.g., magnetic audio- and video-tapes). It may be an original or a copy;

[5] Deleberazione n. 11 del 19 febbraio 2004 del Centro Nazionale per l'Informatica nella Pubblica Amministrazione: "Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformita' dei documenti agli originali". These technical rules derive from the provisions of DPR 445/2000, art. 6, par. 2, and replace the previous ones issued by AIPA with Deliberation no. 42 of 13 December 2001.

c) “Original analog document”: analog document that may be the only existing one or not if, in this case, one can know its content by means of other documents whose preservation is mandatory, even if they belong to different owners;
d) “Electronic document”: the electronic configuration of acts, facts or data which are legally relevant;
e) “Storage digital medium”: physical medium which allows electronic documents storage by means of laser technology (such as, for instance, optical disks, magnetic-optical disks, DVD);
f) “Storing”: process of transposition of analog or electronic documents, signed ones included, on to any suitable medium through processing them;
g) “Electronic archiving”: process of storing electronic documents, signed ones included, on any suitable medium. Documents must be uniquely identified by means of a reference code before any possible preservation process;
h) “Archived document”: electronic documents, signed ones included, which has been subjected to the process of electronic archiving;
i) “Substitute preservation”: process carried out according to arts. 3 and 4 of this deliberation;
l) “Preserved document”: document subjected to the process of substitute preservation;
m) “Exhibiting”: operation which allows visualizing a preserved document and making a copy;
n) “Direct copying”: process of transferring one or more preserved documents from a storage digital medium to another one, without altering their electronic configuration *[conversion?]*. For such a process, no special procedures are provided;
o) “Substitutive copying”: process of transferring one or more preserved documents from a storage digital medium to another one, altering their electronic configuration *[migration?]*. For such a process, special procedures are provided as to arts. 3 and 4 of this deliberation;
p) “Time reference”: information about day and time which is associated to one or more electronic documents;
q) “Public officer”: notary or other authorized officers;
r) “Electronic string”: bit string that can be elaborated through an electronic procedure;
s) “Message digest”: predefined length bit string that is generated by applying a proper hash function to the string;
t) “Hash function”: mathematical function that, starting from a generic bit string, generates a message digest in such a way that it would actually be impossible, starting from the latter, to determine a bit string which could generate it, as well as it would be impossible to determine a pair of bit strings for which the hash function could generate two identical message digests;
u) “Digital signature”: as defined in DPR 445/2000, art. 1 and following amendments.

CNIPA’s Del. 11/2004, art. 2
Substitute preservation obligations:

1. The obligations concerning documents substitute preservation, which are provided by the current legislation as regards both public administrations and private entities, are

fulfilled for any legal purpose when the preservation process is carried out according to arts. 3 and 4.

2. Electronic documents, signed ones included, can be electronically archived before undergoing the preservation process. This deliberation does not provide any obligations as regards electronic archiving.

CNIPA's Del. 11/2004, art. 3
Substitute preservation of electronic documents:

1. The process of substitute preservation of electronic documents, signed ones included, and, in case, of their digests as well, consists in storing them on digital media and ends with affixing time reference and digital signature of the person responsible for preservation, testifying the proper execution of the process, on the whole of the documents or on an electronic string containing one or more digests of those documents or groups of them.

2. The process of substitute copying *[migrating]* preserved electronic documents consists in storing them on another digital medium and ends with affixing time reference and digital signature of the person responsible for preservation, testifying the proper execution of the process, on the whole of the documents or on an electronic string containing one or more digests of those documents or groups of them. Additionally, if the process concerns signed electronic documents, a public officer is required to affix time reference and digital signature, in order to testify that what has been copied *[migrated]* is a true copy.

CNIPA's Del. 11/2004, art. 4
Substitute preservation of analog documents:

1. The process of substitute preservation of analog documents consists in directly storing the relevant image and, in case, the relevant digest as well, on digital media and ends with affixing time reference and digital signature of the person responsible for preservation, testifying the proper execution of the process, on the whole of the documents or on an electronic string containing one or more digests of those documents or groups of them.

2. The process of substitute preservation of original and sole analog documents ends with further affixing of time reference and digital signature of a public officer, in order to testify that what has been copied is a true copy.

3. Destruction of analog documents whose preservation is mandatory is only allowed after completion of the substitute preservation procedure.

4. The process of substitutive copying *[migrating]* preserved analog documents consists in storing them on another digital medium. When copying *[migration]* is completed, the person responsible for preservation testifies the proper execution of the process through affixing time reference and digital signature on the whole of the documents or on an

electronic string containing one or more digests of those documents or groups of them. If the process concerns original and sole documents, a public officer is further required to affix time reference and digital signature, in order to testify that what has been copied is a true copy.

CNIPA's Del. 11/2004, art. 5
Tasks and responsibilities of the person in charge of the preservation function:

a) To specify the features and requirements of the preservation system according to types of documents (analog or electronic) to be preserved. To consequently organize the digital media content and to manage the security and tracking procedures which assure proper preservation, with also the purpose to allow exhibiting of each preserved document;
b) By employing specific processing procedures according to the kinds of storage media utilized, to archive and make available the following information:
   1) content description of the whole of the documents *[i.e., series description]*;
   2) data which identify the person responsible for preservation;
   3) if it is the case, data which identify the persons delegated by the responsible for preservation, with the indication of their tasks; and
   4) information about security copies.
c) To maintain and make accessible a data bank of the software applications in use in all their different versions;
d) To check proper functioning of the system and applications in use;
e) To take the necessary measures to guarantee the physical and logical security of the system which manages the substitute preservation process, as well as of the security copies of storage media;
f) To ask for public officer's assistance, when that is required *[In PAs, the public officer's role is performed by the top manager in charge of the office responsible for the preservation function – art. 5, par. 4]*;
g) To identify and document the safety measures to be observed as regards time reference affixing;
h) To check periodically, at least every 5 years, whether the preserved documents are actually readable, and, when necessary, to provide for direct or substitute copying of the content of the media.

CNIPA's Del. 11/2004, art. 6
Exhibiting obligation:

1. Preserved documents should be readable at any time through the substitute preservation system as well as be available on paper upon request.

2. Preserved documents may also be exhibited via telecom tools.

3. Every time preserved documents are exhibited on paper outside the place where the substitute preservation system is located, a public officer has to testify their authenticity, in case the preservation of those documents requires his or her intervention.

CNIPA's Del. 11/2004, art. 8
Other storage media:

1. Taking technological developments into considerations and according to the DPR 445/2000, public administrations and private entities are allowed to use any kind of storage medium, not necessarily a digital one, which must however be suitable for guaranteeing that copies are true copies, in both substitute preservation and substitute copying *[migration]* processes.

- EUROPEAN UNION -

Council Resolution of 6 May 2003 on Archives in the Member States (2003/C 113/02)

The Council of the European Union:
(…)
8. Invites the Commission to convene a group of experts (…) to address the following:
(…)
c) promotion of concrete activities, such as:
- the strengthening of Europe-wide collaboration on the authenticity, long-tem preservation and availability of electronic documents and archives. (…)

Directive of European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures (1999/93/EC)

Exposition:
(…)
(4) Electronic communication and commerce necessitate " electronic signatures" and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States may create a significant barrier to the use of electronic communications and electronic commerce; on the other hand, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies; legislation in the Member States should not hinder the free movement of goods and services in the internal market;
(5) The interoperability of electronic-signature products should be promoted;
(…)
(8) Rapid technological development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically;
(9) Electronic signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures;
(…)
(11) 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;
(12) Certification services can be offered either by a public entity or a legal or natural person, when it is established in accordance with the national law; whereas Member States should not prohibit certification-service-providers from operating outside voluntary accreditation schemes; it should be ensured that such accreditation schemes do not reduce competition for certification services;
(13) Member States may decide how they ensure the supervision of compliance with the provisions laid down in this Directive; this Directive does not preclude the establishment of private-sector-based supervision systems; this Directive does not oblige certification-service-providers to apply to be supervised under any applicable accreditation scheme;
(…)
(16) This Directive contributes to the use and legal recognition of electronic signatures within the Community; a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; the legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognised;
(17) This Directive does not seek to harmonise national rules concerning contract law, particularly the formation and performance of contracts, or other formalities of a non-contractual nature concerning signatures; for this reason the provisions concerning the legal effect of electronic signatures should be without prejudice to requirements regarding form laid down in national law with regard to the conclusion of contracts or the rules determining where a contract is concluded;
(18) The storage and copying of signature-creation data could cause a threat to the legal validity of electronic signatures;
(19) Electronic signatures will be used in the public sector within national and Community administrations and in communications between such administrations and with citizens and economic operators, for example in the public procurement, taxation, social security, health and justice systems;
(20) Harmonised criteria relating to the legal effects of electronic signatures will preserve a coherent legal framework across the Community; national law lays down different requirements for the legal validity of hand-written signatures; whereas certificates can be used to confirm the identity of a person signing electronically; advanced electronic signatures based on qualified certificates aim at a higher level of security; advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device can be regarded as legally equivalent to hand-written signatures only if the requirements for hand-written signatures are fulfilled;
(21) In order to contribute to the general acceptance of electronic authentication methods it has to be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States; the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorisation of the certification-service-provider involved; national law governs the legal spheres in which electronic documents and electronic signatures may be used; this Directive is without prejudice to

the power of a national court to make a ruling regarding conformity with the requirements of this Directive and does not affect national rules regarding the unfettered judicial consideration of evidence;
(22) Certification-service-providers providing certification-services to the public are subject to national rules regarding liability;
(23) The development of international electronic commerce requires cross-border arrangements involving third countries; in order to ensure interoperability at a global level, agreements on multilateral rules with third countries on mutual recognition of certification services could be beneficial;
(24) In order to increase user confidence in electronic communication and electronic commerce, certification-service-providers must observe data protection legislation and individual privacy;
(25) Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Community or national law;
(…)

Art. 2
Definitions

1. "Electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;
2. "Advanced electronic signature" means an electronic signature which meets the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
3. "Signatory" means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;
4. "Signature-creation data" means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;
5. "Signature-creation device" means configured software or hardware used to implement the signature-creation data;
6. "Secure-signature-creation device" means a signature-creation device which meets the requirements laid down in Annex III;
7. "Signature-verification-data" means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;
8. "Signature-verification device" means configured software or hardware used to implement the signature-verification-data;
9. "Certificate" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;
10. "Qualified certificate" means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II;

11. "Certification-service-provider" means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;
12. "Electronic-signature product" means hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;
13. "Voluntary accreditation" means 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.

Art. 5
Legal effects of electronic signatures

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:
(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
(b) are admissible as evidence in legal proceedings.

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
- in electronic form, or
- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service-provider, or
- not created by a secure signature-creation device.

Art. 6
Liability

1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:
(a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;
(b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;

(c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;
unless the certification-service-provider proves that he has not acted negligently.

2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.

3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate, provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.

4. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties.
The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded.

Art. 8
Data protection

2. Member States shall ensure that a certification-service-provider which issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject.

3. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name.

ANNEX I
Requirements for qualified certificates

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

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

ANNEX II
Requirements for certification-service-providers issuing qualified certificates

Certification-service-providers must:
(a) demonstrate the reliability necessary for providing certification services;
(b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
(c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;
(d) 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;
(e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in 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;
(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;
(g) 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;
(h) 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;
(i) 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;
(j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;
(k) 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 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.

ANNEX III
Requirements for secure signature-creation devices

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
(a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
(b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
(c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

ANNEX IV
Recommendations for secure signature verification

During the signature-verification process it should be ensured with reasonable certainty that:
(a) the data used for verifying the signature correspond to the data displayed to the verifier;
(b) the signature is reliably verified and the result of that verification is correctly displayed;
(c) the verifier can, as necessary, reliably establish the contents of the signed data;
(d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;
(e) the result of verification and the signatory's identity are correctly displayed;
(f) the use of a pseudonym is clearly indicated; and
(g) any security-relevant changes can be detected.