Presidential Decree No. 513 of 10 November 1997

"Regulations establishing criteria and means for implementing Section 15(2)of Law No. 59 of 15 March 1997 concerning the creation, storage and transmission of documents by means of computer-based or telematic systems"

PART I
General Principles

Section 1
(Definitions)

1. With respect to this decree it is defined:

a. "Electronic document" the computer-based representation of legally relevant acts, facts or data.
b. "Digital signature" means the result of a computer-based process (validation) implementing an asymmetric cryptographic system consisting of a public and a private key, whereby the signer asserts, by means of the private key, and the recipient verifies, by means of the public key, the origin and integrity of a single electronic document or a set of such documents.
c. "Validation system" means a computer-based cryptographic system capable of creating and affixing digital signatures or of verifying the validity of digital signatures.
d. "Asymmetric keys" means a pair of cryptographic keys comprising a public and a private key, related to each other, to be used for the encryption or validation of electronic documents.
e. "Private key" means the item within an asymmetric key pair, that is meant to be known only to the holder of the asymmetric keys, and that is used to affix a digital signature to electronic documents or to decrypt electronic documents previously encrypted by means of the corresponding
f. "Public key" means the item, within an asymmetric key pair, that is meant to be made public and that is used to verify the digital signature affixed to electronic documents by the holder of the asymmetric keys, or to encrypt electronic documents for transmission to the holder of the asymmetric keys.
g. "Biometric key" means a string of computer-based codes used in security systems that verify personal identity by reference to physical features unique to the user.
h. "Certification" means the result of a computer-based process that is applied to the public key and that can be detected by validation systems, whereby the public key is certified unique to its holder, the holder is identified, and the period of validity of the key and the expiry date of the corresponding certificate are set, for a period not exceeding three years.
i. "Validation by time-stamp" means the result of a computer-based process under which one or more electronic documents are marked with a date and time that are legally valid against third parties.
j. "Electronic address" means the identifier of a logical or physical resource that is capable of receiving and recording electronic documents.
k. "Certification authority" means the public or private entity that effects the certification, issues the public key certificate, makes the public key and the corresponding certificate publicly available, and publishes and updates certificate suspension and revocation lists.
l. "Revocation of a certificate" means the permanent invalidation of a certificate by the certifying authority as from a specific point in time, excluding retroactive invalidation.
m. "Suspension of a certificate" means the temporary invalidation of a certificate by the certifying authority.
n. "Validity of a certificate" refers to the fact that the information recorded in a certificate is legally valid and invocable against the holder of the corresponding public key.
o. "Technical rules" means technical specifications, including any legal provision to be applied to them.

Section 2
(Electronic documents)

1. Electronic documents, formed by anybody, their computer-based storage and their transmission over telematic systems shall be legally valid and relevant if they are in accordance with the provisions set out in this regulation.

Section 3
(Requirements concerning electronic documents)

1. Technical rules for creating, transmitting, storing, duplicating, reproducing and validating electronic documents, by methods including time-stamping, shall be enacted by decree of the President of the Council of Ministers within180 days from the entry into force of this regulation, having regard to the opinion of the Authority for Information Technology in Public

Administration (AIPA).

2. The technical rules referred to in subsection 1 shall be brought into line with the requirements of scientific and technical progress at least every two years following the entry into force of this regulation.
3. The decree referred to in subsection 1 shall also establish technical, organisational and managerial rules with a view to ensuring the integrity, availability and privacy of the information contained in electronic documents, including situations when biometric keys are used.
4. This regulation shall be without prejudice to the provisions set out in Section 15 of Law No.675 of 31 December 1996.

Section 4
(Writing)

1. Electronic documents that are in accordance with the provisions set out in this regulation shall be regarded as meeting the legal requirement of writing.
2. Ways and means of fulfilling tax obligations relating to electronic documents or their reproduction on any medium shall be established by the Minister of Finance (*Ministro delle Finanze).*

Section 5
(Evidential weight of electronic documents)

1. Electronic documents signed with a digital signature pursuant to Section 10 shall have the evidential weight of a private deed as set out in Section 2702 of the Civil Code.
2. Electronic documents that are in accordance with the provisions set out in this regulation shall have the evidential weight provided for under Section 2712 of the Civil Code and shall satisfy the requirements referred to in Sections 2214 *et seq.* of the Civil Code or in any other equivalent statutory or regulatory provision.

Section 6
(Copies of acts and documents)

1. Duplicates, copies or abstracts of electronic documents, if they are in accordance with the provisions set out in this regulation, shall be valid and relevant for any purpose in law, including situations when they are reproduced on different media.
2. Electronic documents containing a copy or reproduction of public or private deeds or any other document, including all types of administrative acts and records, when sent or issued by the authorised public repository or public official, shall be fully valid for the purposes set out in Sections 2714 and 2715 of the Civil Code, on condition that the digital signature of the sender or issuer has been affixed to or other wised associated with them in accordance with this regulation.
3. Computer-based copies of documents originally produced on paper, or on another non-electronic medium, may substitute for their respective originals for all purposes in law, on condition that they are certified true to the original by a notary public or an authorised public official by means of a statement inserted into the electronic document and legalised as set out in the decree referred to in Section 3(1).
4. The holding of copies and documents sent or issued pursuant to subsection 2 shall confer exemption from the obligation to produce and disclose the paper-based original, whenever such original is required for any purpose in law.
5. Existing legal requirements to retain or disclose acts shall be considered satisfied for all legal purposes by electronic documents, on condition that the processes used are in accordance with the technical rules to be established pursuant to Section 3.

Section 7
(Deposit of the Private Key)

1. The holder of an asymmetric key pair may deposit the private key under secrecy with a notary public or another authorised public repository.
2. The private key to be deposited shall be recorded on any suitable medium by the owner. It shall be delivered in a sealed package such that the information recorded cannot be read, extracted or be otherwise made known without causing alterations or breakage.
3. The deposit shall take place in accordance with the provisions set out in Section 605 of the Civil Code, insofar as these are applicable.

Section 8
(Certification)

1. Any person or entity intending to utilise, for the purposes provided for in Section 2, an asymmetric cryptographic system shall obtain a suitable key pair. One of these keys shall be made publicly available by means of the certification process carried out by a certifying authority.

2. Public keys shall be kept by the certifying authority for at least 10years from the date of publication. They shall be accessible by telematic means as from the beginning of their period of validity.
3. Without prejudice to the provisions of Section 17, the certification operations shall be conducted by certifying authorities named, following notification prior to the beginning of operation, in a public list accessible by telematic means. The list shall be drawn up, maintained and updated by the AIPA. Certifying authorities shall fulfil the following requirements, to be further specified in the decree referred to in Section 3:
    a. Certifying authorities that are private entities shall be set up as *società per azioni;* their registered capital shall meet at least the working capital requirements for authorised banking enterprises;
    b. Legal representatives and administrators of certifying authorities shall meet the requirements of good repute laid down for persons in executive, managerial or auditing positions in banks;
    c. Assurance must be given that the certifying authority's responsible technical staff and staff charged with carrying out certification procedures are sufficiently knowledgeable and proficient to satisfy the provisions set out in this regulation and the technical rules referred to in Section 3;
    d. The quality of computer-based processes and products shall meet internationally recognised standards.
4. The certification process referred to in subsection 1 may also be carried out by a certifying authority whose license or authorisation was issued, subject to equivalent requirements, by another member State of the European Union or European Economic Area.

Section 9

(Obligations on subscribers and certifying authorities)

1. Any person or entity intending to make use of an asymmetric key or digital signature system shall take all necessary organisational and technical measures to prevent loss or damage to third parties.
2. The certifying authority shall:
    a. Accurately identify the person applying for certification;
    b. Issue and publish certificates meeting the requirements to be set out in the decree referred to in Section 3;
    c. On request of the subscriber, and with the assent of the third party concerned, specify any power of representation or other title relating to the subscriber's profession or office held.
    d. Meet the technical rules referred to in Section 3;
    e. Provide exhaustive and clear information to the applicants concerning the certification practice and the technical requirements necessary to obtain certification;
    f. Comply with provisions concerning the minimal security standards of computer systems and the treatment of personal data, according to Section15 (2) of Law No.675 of 31 December 1996;
    g. Not accept the deposit of private keys;
    h. Promptly revoke or suspend certificates in the following circumstances: on request of the subscriber or of the third party of whom the subscriber is an authorised agent; in case the key has been compromised; on decision of an authority; on disclosure of facts limiting the subscriber's capacity; if abuse or forgery is suspected;
    i. Immediately make public any revocation or suspension of an asymmetric key pair;
    j. If the certification activity is discontinued and records are consequently invalidated or transferred to another certifying authority, immediately notify the AIPA and the subscribers, at least six months in advance.

PART II

Digital signature

Section 10

(Digital signature)

1. A digital signature may be affixed or associated by means of a separate document to any electronic document, set of electronic documents, on copies or duplicates thereof.
2. Affixing a digital signature to an electronic document or associating one with it shall have the same effects as putting the required signature to acts or documents written or paper.
3. Any digital signature must uniquely identify a single entity and the document or documents to which it has been affixed or with which it has been associated.
4. The private key used to generate a digital signature must correspond to a public key that is still within its period of validity and that has not been revoked or suspended by the public or

private entity that carried out the certification.

5. Using a digital signature affixed or associated by means of a revoked, suspended or expired key shall have the same effects as failure to sign. Revocation and suspension, whatever the reason, shall take effect on the moment of publication, unless the revoking authority or the entity requesting suspension proves that revocation or suspension was already known to all interested parties.
6. Affixing a digital signature shall, for all purposes in law, complement and substitute for any required seal, stamp, countersign or other distinctive mark.
7. By means of the methods and techniques to be specified in the decree referred to in Section 3, a digital signature must disclose such elements as are sufficient to identify the subscriber, the authority that carried out the certification, and the repository where it is accessible for consultation.

Section 11

(Contracts drawn up by means of computer-based or telematic systems)

1. Contracts drawn up by means of computer-based or telematic systems and digitally signed in accordance with the provisions of this regulation shall be valid and relevant for all purposes in law.
2. Contracts referred to in subsection 1 shall fall within the scope of Legislative Decree No. 50 of 15 January 1992.

Section 12

(Document transmission)

1. It shall be presumed that electronic documents transmitted over telematic systems to the electronic address declared by the recipient have been sent and have reached the addressee.
2. The date and time of creation, transmission or reception of electronic documents produced in accordance with this regulation and with the technical rules referred to in Section 3 shall be legally valid and invocable against third parties.
3. Telematic transmission of electronic documents by methods that ensure reception shall have the same effects as notification by post when such is provided for in law.

Section 13

(Secrecy of telematic correspondence)

1. Persons in charge of the telematic transmission of acts, data or documents created by means of computer- based systems shall not read telematic correspondence, duplicate by any means, pass on or otherwise transfer to third parties any information concerning the existence or content of correspondence, communications or messages transmitted over telematic systems, including summarised or partial information, except when such information is by its nature or by the explicit will of the sender intended to be made public.
2. For the purposes of this regulation, and with regard to operators of information transmission systems, any acts, data and documents transmitted over telematic systems shall be regarded as remaining the property of the sender until delivered to the addressee.

Section 14

(Electronic payment)

1. The transfer of electronic payments between private entities and/or Public agencies shall take place in accordance with the technical rules to be established in the decree referred to in Section 3.

Section 15

(Books and records)

1. Where books, lists and records are required to be kept, they may be created and maintained on a computer-based medium in accordance with this regulation and with the technical rules to be established in the decree referred to in Section 3.

Section 16

(Authenticated and digital signature)

1. A digital signature authenticated by a notary public or another authorised public official shall be deemed to be an authenticated signature for the purposes of Section 2703 of the Civil Code.
2. In order to authenticate a digital signature, the public official shall certify that the digital signature was affixed by the signer in the presence of the official following verification of the signer’s identity and the validity of the public key; that the signed document reflects the signer’s will, and that it is not in breach of existing law, as provided for in Section 28(1) of Law No. 89 of 16 February 1913.
3. The public official’s digital signature shall, for all purposes in law, complement and substitute for any seal, stamp, countersign or other distinctive mark that may be required.
4. Where an electronic document must be accompanied by another document originally created

on a different medium, the public official may attach a certified true electronic copy instead; the original shall be retained by the public official; it shall be annotated with a mention of the document's use and with information identifying the electronic document to which the copy was attached.

5. Digital signatures inserted into electronic documents delivered to or deposited with a Public agency shall be regarded as having been affixed in the presence of the responsible agent, as required for the purposes of Section 3(11) of Law No.127 of 15 May 1997.
6. Documents delivered to or deposited with a Public agency over telematic systems or on a computer-based medium shall be valid, for all purposes in law, on condition that they have been digitally signed and validated by time-stamp in accordance with this regulation.

Section 17

(Cryptographic keys held by Public agencies)

1. In accordance with their statutes, Public agencies shall, on their own authority, generate, store, certify and use their own public keys.
2. The decree referred to in Section 3 shall establish methods by which Public agencies shall generate, publish, store, certify and use their own public keys.
3. The public keys of public officials not employed in Public agencies shall be autonomously certified and published, in accordance with the relevant laws and regulations governing the use of hand-written signatures.
4. Public keys held by legally recognized Professional registers and Bars (*Ordini* and *Albi professionali)* or their legal representatives shall be certified and published by the Ministry of Justice(*Ministro di Grazia e Giustizia)* or by delegated agents.

Section 18

(Electronic documents of the public administration)

1. Public agencies' records created by means of computer-based systems, electronic data and documents are original and primary information that may be copied and reproduced on a variety of media for all purposes provided for in law.
2. All operations relating to the creation, inputting, storage, reproduction and transmission of data, documents and acts by means of telematic or computer systems, including the issuance of administrative acts by means of such systems, shall include easily detectable information identifying the agencies involved and the entity carrying out the operation.
3. The AIPA shall, in consultation with the State Archive Service *(Archivi di Stato)* and, for the classified material, on consultation with the Ministry of Defence *(Ministero della Difesa)*, the Ministry of Finance *(Ministero delle Finanze)*, the Ministry of Interior *(Ministero dell'Interno)*, adopt technical rules for the creation and storage of the electronic documents of Public agencies.

Section 19

(Signature of electronic documents of the public administration)

1. A digital signature shall substitute, in accordance with this regulation, for a hand-written or otherwise required signature in all electronic documents of Public agencies.
2. The use of a digital signature shall, for all purposes in law, complement and substitute for any required seal, stamp, countersign or other distinctive mark.

PART III
Implementation

Section 20

(Development of public administration information systems)

1. By 31 March 1998 Public agencies shall adopt a plan for the development of automated information systems implementing this regulation and in accordance with the technical rules to be established by the AIPA.
2. Within five years from 1 January 1998, Public agencies shall put into place, or review, information systems aimed at fully automating the creation, management, dissemination and use of their data, documents, procedures and acts in accordance with this regulation, the technical rules to be established by the AIPA, and the provisions set out in Laws Nos. 675 and 676 of 31 December 1996.
3. By 31 December 1998, Public agencies shall conduct a cost/benefit analysis to determine whether to convert to a computer-based medium any paper documents or acts whose maintenance is desirable or required; they shall devise the necessary plans to replace paper files by computer-based ones.

Section 21

(1 Computer-based management of document flows)

1. By 31 December 1998, Public agencies shall provide for the computer-based maintenance of internal acts and document management in order to facilitate immediate document retrieval,

ensure availability of files, and make possible telematic access by other Public agencies and authorised private entities to administrative acts.

Section 22

(Forms and questionnaires)

1. By 31 December 1998, Public agencies shall devise, and provide for telematic access to, legally valid electronic forms to be used in data exchanges within the public administration unified network and with private entities.