Technical Annex to the Prime Minister decree of 8 February, 1999.

Technical rules for the creation, transfer, storage, duplication, reproduction and validation, including by time-stamp, of electronic documents, pursuant to the provisions of Section 3 (1) of the Presidential Decree No. 513 of 10 November, 1997.

TITLE I
Basic technical rules

Section 1 – Definition

1. Within these rules the definitions contained in Section 1, Presidential Decree No. 513 of 10 November, 1997, are applied. In addition:

   a. "holder" of a pair of asymmetric keys means the subject, that is assigned to the digital signature produced by the private key of the pair, or the responsible for the service or function that uses the signature by means of automatic devices;
   b. “fingerprint” of a sequence of binary symbols means an additional sequence of binary symbols of pre-defined length, created by applying the appropriate hash-function to the initial sequence;
   c. “hash-function” means a mathematical function that creates, starting from a generic sequence of binary symbols, a fingerprint such that it is practically impossible, starting from that fingerprint, to obtain a sequence of binary symbols creating the same fingerprint value. Moreover it shall be practically impossible to identify two sequences of binary symbols for which the function will create the same fingerprint value;
   d. “signature device” means an electronic device programmable only at the origin, it is part of the validation system and is capable at least to protect private keys and to produce digital signatures inside it;
   e. “computer evidence” means a sequence of binary symbols that can be elaborated by a computer procedure;
   f. “time-stamp” means a computer evidence that can be used to effect temporal validation;

Section 2 – Algorithms for the production and verification of digital signatures

1. The following algorithms shall be used in order to produce and verify digital signatures:

   a. RSA (Rivest-Shamir-Adleman algorithm).
   b. DSA (Digital Signature Algorithm).

Section 3 – Hash algorithms

1. Fingerprints shall be produced by means of one of the following hash-functions, as defined in Regulation ISO 10118-3:

   a. Dedicated Hash-Function 1, corresponding to function RIPEMD-160;
   b. Dedicated Hash-Function 3, corresponding to function SHA-1.

Section 4 – General characteristics of keys

1. A pair of keys shall be assigned to only one holder.

2. If the signature of one holder is affixed using an automatic procedure, a different key, among those owned by the holder, shall be used.

3. If the automatic procedure uses several devices in order to affix the signature of the same holder, a different key for each device shall be used.

4. Within this decree the keys and the related services are sub-divided into the following categories:

a. signature keys: used to create and to verify signatures affixed to or associated with documents;
b. certification keys: used to affix signatures to certificates and to revocation list (CRL) or suspension list (CSL);
c. time-stamp keys: used to create time-stamps.

5. The key shall not be used for any purpose different from which it is intended.

6. Minimum key length shall be 1024 bits.

7. The certification authority shall determine the expiry date of the certificate and the period of validity of the keys in accordance with the used algorithm, length of the keys and the services for which they are intended.

Section 5 – Generation of keys

1. Key pairs shall be generated using systems and procedures which offer, according to the current state of the scientific and technologic knowledge, the uniqueness and strength of the generated key pair and the secrecy of the private key.

2. The key production system must ensure:

   a. the conformity of the key pair to the requirements of the used production and verification algorithms;
   b. the equal probability of producing any of the possible pairs of keys;
   c. the unequivocal identification of the subject that activates the production procedure.

3. The conformity of key production devices to the requirements of this section shall be verified according to the E3 ITSEC criteria with HIGH strength of mechanism or better.

Section 6 – Methods for the generation of keys

1. The creation of the certification and time-stamp keys shall be done only by the same responsible person of the service that will use these keys.

2. The signature keys shall be generated by the holder or by the certifier.

3. The creation of the signature keys made by the holder shall be done inside the signature device.

Section 7 – Generation of keys outside the signature device

1. If the generation of keys is done by a system different from that one dedicated at using the private key, the creation system shall assure:

   a. the impossibility of intercepting or discovering of any information, even temporary, produced during the procedure;
   b. maximum security in transferring the private key into the signature device in witch it will be used.

2. The creation system shall be isolated, exclusively dedicated at this task and adequately protect against risks of interference and interception.

3. The access to the system shall be controlled and each user shall be identified. Every system session shall be recorded in the log-book.

4. Before the creation of a new key pair, the entire system shall proceed to the validation of its own configuration, to the authenticity and integrity of the installed software and to the absence of non authorised programs.

5. The conformity of the system to the requirements of this section shall be verified according to the E3 ITSEC criteria with HIGH strength of mechanism or better.

Section 8 – Storage of keys

1. Private keys are to be stored inside the signature device. The same device may be used to store more than one key.

2. It is forbidden to duplicate the private key or the devices in which it is stored.

3. In order to achieve particular security the key may be sub-divided into several signature devices.

4. The holder of the key shall:

    a. store the private key and the device in which it is put with utmost care to ensure integrity and confidentiality;
    b. keep the activation data for the use of the private key in a different place from that in which the device containing the key is;
    c. request immediate revocation of all certificates associated with a key contained in a lost or defective device.

Section 9 – Format of signatures

1. Signatures produced in accordance with the rules enforced in this decree must comply with regulations issued by bodies, well known from a national or international point of view, or with public specifications (Public Available Specification – PAS).

2. The certificate with the public key to be used for verification purpose must be enclosed to the signature.

Section 10 – Generation and verification of signatures

1. The systems and the procedures used to generate, to affix and to verify digital signatures must display the data to which the signature is to be affixed in a clear and unambiguous manner. They must ask for confirmation of the will to produce the signature.

2. The ss (1) above does not apply to signature produced using an automatic procedure provided that the starting of the procedure is clearly identified with the will of the signer.

3. Signatures shall be produced inside a signature device that makes impossible to intercept the value of the private key.

4. The signature device shall identify the holder prior to signature production.

5. The conformity to the requirements of this decree of the systems used to create signatures is to be verified according to the E3 ITSEC criteria with HIGH strength of mechanism or better.

6. The conformity to the requirements of this decree of the systems used to verify signatures is to be verified according to the E2 ITSEC criteria with HIGH strength of mechanism or better.

Section 11 – Information contained in certificates

1. Each certificate shall contain the following information:

    a. the series number of the certificate;
    b. the business name of the certification authority;
    c. the identification code assigned to the holder by the certification authority;
    d. the first name, surname and date of birth or the business name of the holder;
    e. the value of the public key;

f. applicable production and verification algorithms;
g. the commencement and expiry dates of the validity period of the key pair;
h. algorithm of certificate request.

2. The key typologies must unequivocally be deduced by the certificate.

3. If the certificate is issued in respect of a pair of signature keys, the following information shall be provided in addition to that described in ss (1) above:

   a. any restrictions on the use of the pair of keys;
   b. any representative powers;
   c. any professional certification.

4. If the certificate is issued in respect of a pair of certification keys, the key usage for certification must be provided in addition to that described in ss (1) above.

5. If the certificate is issued in respect of a pair of time-stamp keys, the following information shall be provided in addition to that described in ss (1) above:

   a. key usage for time-stamp;
   b. identification code of the time-stamp system in which the keys will be used.

Section 12 – Format of certificates

1. Certificates and related revocation lists shall comply with the standard ISO/IEC 9594-8:1995 with extensions defined in Variant 1, or with Public Specification PKCS#6 e PKCS#9 and their modifications and integration.

Section 13 – Procedures governing access to the register of certificates

1. The access to the register of certificates kept by each certification authority may be done in accordance with procedures compatible with the LDAP protocol as defined in public specification RFC 1777.

2. The certification authority shall be free to provide other methods of access to the register certificates in addition to those specified in ss (1) above.

3. Each certification authority shall publish the electronic addresses and telephone numbers which permit access to the register at least in the public list as described in Section 8(3) of Presidential Decree No. 513 of 10 November, 1997.

TITLE II
Rules governing the Certifications of keys

Section 14 – Keys for the Authority responsible for Information Technology in Public Administration bodies (AIPA)

1. The AIPA may delegate certification of its own keys to the “Technical Centre for assistance to bodies using the unitary network of the Public Administration” (“Centro Tecnico per la RUPA”), established in compliance with Section 17(19) of the law No. 127 of 15 May 1997.

2. For each pair of keys, the Official Gazette of the Italian Republic shall publish one or more identification codes to be used in order to verify the value of the public key.

Section 15 – Public list of certification authorities

1. The public list of certification authorities which the AIPA is expected to keep and update according to Section 8(3) of Presidential Decree No. 513 10 November, 1997 shall specify the following information for each certification authority:

    a. Business name,
    b. Registered office,
    c. Legal representative,
    d. Name X.500,
    e. Internet address,
    f. List of telephone numbers required for access,
    g. List of certificates for the certification keys,
    h. Operating manual,
    i. Date of cessation of activity and substitute certification authority.

2. The public list shall bear the signature of the AIPA.

Section 16 – Request for inclusion in the public list of certification authorities

1. Anyone wishing to conduct the business of certification authority shall submit to the AIPA a request for inclusion in the public list as described in Section 8(3) of Presidential Decree No. 513 of 10 November, 1997. The request shall be in accordance with the procedure to be established by the AIPA in a circular.

2. The following documents are to be enclosed with the request:

    a. a copy of the operating manual;
    b. a copy of the security plan;
    c. a list of the personnel responsible for producing keys, issuing certificates and handling the register of keys;
    d. a copy of the insurance policy covering risks associated with the certification activity and third part liabilities.

3. The AIPA may request supplementary information in addition to the above documents.

4. Within 60 days of the presentation of the request for membership in the public list, the request shall be accepted or denied with justification provided. The request of supplementary information suspends the counting of the maturity date.

5. The “Technical Centre for assistance to bodies using the unitary network of the Public Administration” (“Centro Tecnico per la RUPA”) is a member of the public list of certification authorities with reference to tasks defined in Presidential Decree No. 522, 23 December, 1997. The Technical Centre must comply with the regulations enforced in these technical rules.

Section 17 – Registration in the public list of certification authorities

1. The certification authority whose request for membership has been accepted shall arrange for a system of secure communication with the AIPA in view of the exchanges of information described in this decree.

2. The entity requesting membership shall provide both the information required by Section 15(1) and the certificates for its own certification keys, generated in accordance with the procedure described in Section 19.

3. The entity requesting membership shall produce a certificate of its own for each of AIPA signature keys and include these certificates in its register.

4. The certification authority shall maintain a copy of the list, signed by AIPA, of the certificates related to the certification keys of Section 15(1g). This list shall be available via telecommunication network.

Section 18 – Check for requirement of certification authorities

1. The certification authority shall confirm in written form to the AIPA the possess of its own requirement in order to continue the business after any change of the information of Section 16 or in any case one year after its previous request or confirmation.

2. The absence of one or more requirements of Section 16 will produce the cancellation from the public list.

3. The methods to execute the regulations of this Section are to be established by the AIPA in a circular.

4. AIPA may interact and ask for information to any Public Administration in order to execute the check and control activities described in this Section in compliance to Section 7(4) of law decree No. 39 of 12 February, 1993.

Section 19 – Production of certification keys

1. Certification keys shall be produced in compliance with the requirements of Sections 5, 6 and 7.

2. For each certification key the certification authorities shall produce a certificate to be signed using the private key of the pair to which the certificate refers to.

Section 20 – Cessation of activity

1. A certification authority intending to cease its activities shall give the AIPA at least 6 months' notice specifying a substitute certification authority or repository for the register of certificates and related documentation.

2. The AIPA shall publish the relevant date of cessation in the public list, specifying the name of the substitute certification authority or repository for the register of certificates and related documentation.

3. Within the same six-months period the certification authority shall inform the holders of the certificates it has issued that all certificates still valid will be revoked at the time it ceases business.

Section 21 – Reciprocal certification among certification authorities

1. Certification authorities may enter into agreement providing for their reciprocal certification.

2. Each certification authority shall issue to the other a certificate for each certification key recognised by agreement.

3. The certificate as per ss (2) above must define correspondences between equivalent clauses contained in the operating manuals of the two certification authorities.

Section 22 – Registration of holders

1. In order to obtain certification of a public key the holder must be already registered with the certification authority. The request for registration shall be in written form and shall be retained by the certification authority for a minimum of 10 year term.

2. Upon effecting registration, the certifying authority shall verify the identity of the party making the request. The certification authority shall be free to define its own user identification methods publishing them in the operating manual.

3. The certification authority shall assign a unique identification code to each registered holder. At the same subject may be assigned separate identification codes for each role in respect of which he is authorised to sign.

Section 23 – Use of pseudonyms

1. The data as described in Section 11(1)(d) may be substituted in the certificate by a pseudonym.

2. The fact that a pseudonym is used instead of personal data must be declared in the related certificate.

3. The certification authority shall retain the information pertaining to the real identity of the holder on record for a minimum ten-year term following the expiry of the certificate.

Section 24 – Information to be compulsorily provided

1. The certification authority shall inform the holder about his obligations concerning the preservation of the secrecy of the private key and the correct storage and use of signature devices.

2. The certification authority shall inform the holder about any certification agreement stipulated with other certification authorities as described in Section 21.

Section 25 – Communication between certification authority and holder

1. Upon registration, when the holder does not have other keys that may be used for her or his authentication, the certification authority may provide the holder with the means required to achieve secure communication in conducting the following activities by telecommunication systems:

    a. customisation of signature devices;
    b. request for certification of keys produced outside the certification authority environment;
    c. request for immediate revocation of a certificate.

2. In case of absence of such a telecommunication system the aforementioned operations will have to be carried out on the premises of the certification authority.

Section 26 – Customisation of the signature device

1. The signature device customisation process consists in:

    a. acquisition, by the certification authority, of the identification data of the used signature device and their association with the holder;
    b. recording, inside the signature device, of the holder's identification data on the premises of the certification authority.
    c. recording, inside the signature device, of the certificates issued in respect of the certification authority's key.

2. During the signature device customisation phase the certification authority verifies the good working of the device.

3. The customisation of the signature device is recorded in the log-book.

Section 27 – Certification request

1. The holder who means to obtain the certification of a pair of keys must forward the request, via the communication system in accordance with article 25, or with other mechanism indicated in the operating manual.

2. In the request shall be specified the information which the subject does not want to be inserted in the certificate.

3. The certification request must be conserved by the certification authority for a minimum of 10 year term.

Section 28 – Production of certificates

1. Before emitting the certificate the certification authority must:

    a. check the authenticity of the request;
    b. verify that the public key whose certification is requested has not already been certified by one of the certification authority enrolled in the list;
    c. demand the proof of the possession of the private key and to verify the correct functioning of the pair of keys, eventually demanding the signing of one or more test documents.

2. The request for certification must be rejected if the verification as described in ss (1)(b) above evidences the existence of certificates, relating to the key whose certification is requested, with a holder different from the petitioner. This event must be recorded in the log-book and the subscriber of the key already certified must be informed. If the proof of possession has been supplied in accordance with the ss (1)(c), relating to the key already certified, the procedure of certificate revocation must be started as described in Section 30.

3. The certificate must be generated with a system compliant to the requirements outlined in Section 42.

4. The certificate must be published by means of insertion in the repository managed by the certification authority. The moment of the publication must be attested by means of generation of one time-stamp, that must be conserved until expiration of the keys.

5. The issued certificate and the related time-stamp must be sent to the subscriber.

6. For every issued certificate the certification authority must supply to the subscriber a classified code, to use in case of emergency in order to authenticate an eventual revocation request of the certificate.

7. The production of certificates is recorded in the log-book.

Section 29 – Revocation of certificates relating to signature keys

1. The revocation of a certificate determines the anticipated termination of its validity.

2. Revocation may be effected at request of the holder or of an interested third party as per Section 9(2)(c) of the Presidential Decree No. 513 of 10 November, 1997, or upon the initiative of the certification authority.

3. A certificate is revoked by the certification authority by being included in the applicable list of revoked certificates (CRL) managed by the same. The revocation is effective upon publication of the list containing the same and shall be permanent.

4. The moment of publication of the list must be asserted by the affixing of a time-stamp.

5. If a certificate is revoked on grounds that the secrecy of the private key may have been compromised, the certification authority shall publish an update of the revocations list immediately.

6. Revoked certificates shall be recorded in the log-book.

Section 30 – Revocation upon initiative of the certification authority

1. Except cases of motivated emergency, the certification authority wishing to revoke a certificate must provide notification to the holder, specifying the reasons for revocation and the date and time from which the certificate ceases to be valid.

Section 31 – Revocation at the request of the holder

1. A holder requesting revocation shall submit a written request to such effect specifying the grounds for the revocation and the date and time when the revocation is to be effective.

2. As a rule, the request is forwarded through the secure system of communication as described in Section 25.

3. Other methods for forwarding requests are to be specified by the certification authority in the operating manual.

4. The certification authority shall check the request for authenticity and proceed with the revocation within the requested time limit. Requests forwarded using procedures pursuant to ss (2) shall be considered valid.

5. In case if the certification authority is not in a position to ascertain the authenticity of the request in time, the certificate will have to be suspended.

Section 32 – Revocation at the instigation of an interested third party

1. A request for revocation made by an interested third party pursuant to the provisions of Section 9(2)(c) of Presidential Decree No. 513 of 10 November, 1997 shall be submitted in written form and accompanied by the appropriate supporting documentation.

2. The certification authority must notify the request to the holder.

Section 33 – Suspension of certificates

1. The validity of a certificate may be suspended at the request of the holder, at the instigation of an interested third party as per Section 9(2)(c) of Presidential Decree 513/97 or upon the initiative of the certification authority.

2. Certificates are suspended by being included in one of the lists of suspended certificates. The suspension shall be effective upon publication of the list. The date and the hour of publication are guaranteed from the affixing of one time-stamp.

3. Suspended certificates shall be recorded in the log-book.

Section 34 – Suspension upon the initiative of the certification authority

1. A certification authority wishing to suspend a certificate must provide prior notification to the holder, specifying the reasons for the suspension and its duration.

2. Upon completion of the suspension procedure the holder shall be notified and informed of the date and time the suspension shall go into effect.

3. If the suspension is the result of a request for revocation on grounds that the key may have been compromised, the certification authority must make the suspension public immediately.

Section 35 – Suspension at the request of the holder

1. A holder requiring suspension shall submit a written request for such effect specifying the grounds and the period for which the validity of the certificate is to be suspended.

2. As a rule, the request is forwarded through the secure communication system as described in Section 25.

3. Alternatives methods of submitting requests are to be specified by the certifying authority in the operating manual.

4. The certification authority shall verify the authenticity of the request and proceed with the suspension of the certificate within the specified time period. Requests forwarded in accordance with the procedures indicated in ss (2) above shall be considered valid.

5. In case of emergency the immediate suspension of a certificate may be requested by using the code as described in Section 28(6). The request is to be subsequently confirmed using one of the methods determined by the certification authority.

Section 36 – Suspension at the instigation of an interested third party

1. An interested third party may require suspension of a certificate under the provisions of Section 9(2)(c) of Presidential Decree 513/97 by submitting a request for such effect and enclosing to it the appropriate supporting documentation.

2. The certification authority must notify the request to the holder.

Section 37 – Replacement of the certification keys

1. At least 90 days before the expiry of a certificate related to a certification key, the certification authority shall initiate procedures for its replacement by creating a new pair of key in accordance with the procedure indicated in Section 19.

2. In addition to the certificate as provided in ss (1) above, the certification authority shall generate a certificate for the new public key to be signed with the private key of the old pair and a certificate for the old public key to be signed with the new private key.

3. The certificates generated in accordance with the requirements of ss (1) and ss (2) above shall be supplied to the AIPA, which updates the list as described in Section 15(1)(g) and forwards it to the certification authorities for its publication as provided for in Section 17(4).

Section 38 – Revocation of certificates relating to certification keys

1. Revocation of a certificate relating to a pair of certification keys can be done only in the following cases:

    a. compromise of the secret key;
    b. malfunction in the signature device;
    c. cessation of activity.

2. The revocation shall be notified within 24 hours to the AIPA and to all the holders of certificates that were signed using the secret key of the revoked pair.

3. The revoked certificate is to be immediately included in an updated list of revocations.

4. Only those certificates whose both the related certification key and the key used to produce the time-stamps, as provided in Section 28(4), have been compromised must be revoked.

5. The AIPA shall update the list as provided in Section 15(1)(g) and shall forward it to the certification authorities for its publication as provided in Section 17(4).

Section 39 – Replacement of the AIPA keys

1. The AIPA shall arrange for the creation and certification of a new pair of keys at least 90 days prior to expiry date of the pair of keys it uses for signing items contained in the public list of certification authorities.

2. A copy of the items contained in the public list of certification authorities shall be signed with the new pair of keys.

3. The AIPA shall update the list as provided in Section 15(1)(g) and shall forward it to the certification authorities for its publication as provided in Section 17(4).

Section 40 – Revocation of certificates relating to the AIPA keys

1. Certificates relating to the AIPA keys may only be revoked if the secret key is suspected to have been compromised or the signature device is found to be faulty.

2. In the hypothesis of ss (1), the AIPA shall request to every certification authority the immediate revocation of the certificate issued to it as provided in Section 17.

3. The AIPA shall be responsible for the substitution of the revoked key according to Section 39.

Section 41 – Security requirements of the operating systems

1. The operating system of the processing systems used in certification activities for key generation, for certificate generation and for handling the register of certificates shall comply with the specification indicated in the F-C2/E2 ITSEC class or with TCSEC C2.

2. The requirement as provided in ss (1) above it is not applied to the operating system of the signature device.

Section 42 – Characteristics of the system for the production of certificates

1. Certificates shall be produced using a system dedicated exclusively to this function, located in secure premises.

2. Entry and exit events from secure premises are to be recorded in the log-book.

3. The access to the processing systems shall only be permitted to authorised personnel assigned to specific functions. At the opening of each session the system shall identify such personnel by means of an appropriate identification procedure.

4. The starting and the ending times of each session shall be recorded in the log-book.

Section 43 – Register of certificates

1. The register of certificates contains:

    a. the certificates issued by the certification authority;
    b. the list of revoked certificates;
    c. the list of suspended certificates.

2. The certification authority shall be authorised to sub-divide the list of revoked and suspended certificates into several separate lists.

3. The certification authority shall be authorised to duplicate the register of certificates in more than one site so long as the consistency and integrity of the copies is guaranteed.

4. The register of certificates shall be accessible for any subject in accordance with procedures as established in Section 13.

Section 44 – Requirements applicable to the register of certificates

1. The certification authority must maintain a reference copy of the register of certificates to which the access from outside is to be impossible. The reference register will have to be located in a secure system installed in secure premises.

2. The certification authority shall systematically verify correspondence between the operational copy and the reference copy of the register of certificates. Any lack of correspondence is to be immediately notified and recorded in the operations registry.

3. Operations that modify the content of the register of certificates shall only be effected by personnel specifically authorised.

4. All operations that modify the content of the register are to be recorded in the log-book.

5. The starting and the ending date and time of each period of time over which the register of certificates is not accessible from the outside and those of each period over which its internal functions are not available are to be recorded in the log-book.

6. At least one back-up copy of the operations copy and of the reference copy for the register of certificates shall be kept in separate safety cabinets, located on different premises.

Section 45 – Operating manual

1. The procedures the certification authority intends to adopt in conducting its activity shall be defined in an operating manual.

2. The operating manual shall be lodged with the AIPA and published by the certification authority for consultation by telecommunication means.

3. The minimum information to be provided in the operating manual is as follows:

   a. the identification data of the certification authority;
   b. the identification data of the version of the operating manual;
   c. the name of the person in charge of the operating manual;
   d. a description of the obligations of the certification authority, of the holder and of the persons having access for purpose of signature verification;
   e. definitions of the responsibilities and limitations to compensations, if any;
   f. applicable fees;
   g. the procedure governing the identification and recording of users;
   h. the procedure adopted for creating keys;
   i. the procedure adopted in issuing certificates;
   j. the procedure governing the suspension and revocation of certificates;
   k. the procedure adopted in replacing keys;
   l. the procedure governing the handling of the register of certificates;
   m. the procedure governing the access to the register of certificates;
   n. methods and procedure to safeguard confidentiality;
   o. procedures governing the handling of back-up copies;
   p. accident management procedure.

Section 46 – Security plan

1. The Security representative shall establish a security plan detailing at least the following elements:

   a. the overall structure, operational methods and logistical structure of the organisation;
   b. a description of security infrastructure for each building relevant for the security goals;
   c. the location of services and offices on the premises of the organisation;
   d. a personnel list providing indications as to the location of their offices;
   e. the organisation's accountability matrix;
   f. a description of the cryptographic algorithms used;
   g. a description of the certification procedures adopted;
   h. a description of the installed devices;
   i. a description of the data flows;
   j. the procedure adopted for handling backup copies of data;
   k. disaster recovery procedures;
   l. risk analysis;
   m. description of countermeasures;
   n. specifications of the controls;

2. The security plan shall comply with the requirements of Section 9(2)(f) of the Presidential Decree 513/97 concerning the security of personal data.

Section 47 – Log-book

1. The log-book shall include all the entries which the devices installed on the premises of the certification authority are to effect automatically in connection with the situations as described in this decree.

2. Additional entries may also be made using separate and different types of media.

3. Each entry must be associated with the date and time it was carried out.

4. The log-book must be held in such a way as to preserve the authenticity of the annotations on it. The log-book must permit the accurate reconstruction of any security relevant events occurring in the system.

5. The integrity of the log-book must be checked at least on a monthly basis.

6. Entries contained in the control log shall be stored in accordance with the procedures established by this decree and retained for a minimum ten-year term.

Section 48 – Quality system of the certification authority

1. Within a year from the start of the certification activity, the quality system of the certification authority must be certificate in accordance with ISO 9002 standards.

2. The quality manual shall be lodged with the AIPA and a copy shall be available on the certification authorities premises.

Section 49 –Certification authority's personnel organisation

1. As a minimum requirement, the certification authority's personnel shall include the following functions:

    a. the security representative;
    b. a person responsible for the production and custody of keys;
    c. a person responsible for customisation of signature devices;
    d. a person responsible for the production of certificates;
    e. a person in charge of handling the registry of certificates;
    f. a person in charge of user registration;
    g. a person in charge of data security;
    h. a person in charge of cryptographic;
    i. a person in charge of technical services;
    j. a person in charge of auditing.

2. The same person may be assigned to more of the above tasks as long as they are compatible.

3. The function groups mentioned below shall be considered to be compatible:

    a. production and custody of the keys, production of certificates, customisation of signature devices, cryptography, data security;
    b. registration of users, management of register of certificates, cryptography, data security.

Section 50 – Requirement of good repute for certification authorities

1. The requirement of good repute of the Section 8(3)(b) of Presidential Decree 513/97 are those described in the Decree of the Minister of the Treasury, Budget and Economic Programming, dated March 18, 1998, No. 161.

Section 51 – Requirement in terms of personnel skills and experience

1. Personnel assigned to the functions listed in Section 49, must have at least 5 years' experience in the analysis, design and operation of computer systems.

2. A training course is to be organised in connection with each upgrade of the certification system.

TITLE III
Rules for temporal validation and protection of electronic documents

Section 52 – Temporal validation

1. A "computer evidence" may receive temporal validation using an appropriate time-stamp generated for such purpose.

2. Time-stamps are generated by an appropriate secure electronic system capable of:

    a. permanently maintaining the date and time in compliance with the requirements of this decree;
    b. creating a data structure containing the information specified in Section 53;
    c. placing a digital signature on the data structure as per (b) above.

Section 53 – Information to be provided in time-stamps

1. As a minimum requirement, a time-stamp shall contain the following information:

    a. user identification data of the issuer;
    b. the series number of the time-stamp;
    c. the signature algorithm of the time-stamp;
    d. the identification data of the certificate associated to the stamp verification key;
    e. the date and time the stamp was produced;
    f. identification data of the hash algorithm used in order to generate the fingerprint of the computer evidence subject to time-stamp validation;
    g. the value of the fingerprint of the computer evidence.

2. A time-stamp may also contain data identifying the entity to which the fingerprint relating to ss 1(g) above belongs.

3. The date and time in the time-stamps shall be specified with reference to the UTC universal time.

Section 54 – Time-stamp keys

1. Each pair of keys used for temporal validation is to be uniquely associated with one time-stamp validation system.

2. In order to limit the number of time-stamps generated with the same key pair, the time-stamp keys are to be replaced at least monthly, independently from the duration of their validity period and without revoking the related certificate.

3. Certificates relating to time-stamp keys shall be signed using certification keys different from those used to sign certificates relating to standard signature keys.

Section 55 – Accuracy of temporal validation systems

1. Pursuant to the Decree of the Minister of Industry, Commerce and Craft No. 591 of 30 November, 1993, the time to be assigned to time-stamps upon their production must reflect the UTC (IEN) time scale with a departure therefrom not to exceed one full minute.

Section 56 – Security of temporal validation systems

1. Each temporal validation system must produce an operating registry on a not re-writable medium on which are automatically stored the events for which recording is required based on this decree.

2. Any anomaly or any attempt of tampering that may interfere with the functioning of the apparatus and make it incompatible with the requirement described in this decree, specifically with those of Section 55(1) above, shall be recorded on the operating registry and shall lead to system block.

3. The block of the temporal validation system may be revoked exclusively by personnel specifically authorised.

4. The conformity to the security requirements specified in this Section shall be verified in accordance with the criteria established by ITSEC E2 evaluation level with HIGH strength of mechanism or better. In any case the components used in order to sign time-stamps are subjected to the requirements of Section 10.

Section 57 – Recording of stamps produced

1. All the issued time-stamps are to be stored in an appropriate digital archive until the expiry of the public key of the pair used for their production.

Section 58 – Request for temporal validation

1. The certification authority shall establish the procedures used in order to perform a request for temporal validation and publish them in the operating manual

2. The request shall contain the computer evidence to which the time-stamps must refer to.

3. The computer evidence may be replaced by one or more fingerprints, calculated using hash functions indicated in the operating manual. Hash functions pursuant to Section 3 must in any case be accepted.

4. One request may specify the issue of more than one time-stamps for the same computer evidence. In such a case time-stamps generated with different keys must be obtained.

5. A time-stamps generation service must ensure a response time not exceeding one full minute, measured as the time lag between the time when the service receives a request and the time appearing in the time-stamp.

Section 59 – Protection of electronic documents

1. On demand of the interested subject and exclusively in order to assure the association between the electronic document and the related time-stamps, the certification authority may store a copy of the electronic document which the time-stamps refers to.

2. The storage modalities and the procedures used for requesting the service must be described in the operating manual.

Section 60 – Extension of the validity of an electronic document

1. The validity period of an electronic document may be extended beyond the time limit of the signature key by associating one or more time-stamps to the document concerned.

2. The validity period of an electronic document may be further extended. To this end a new time-stamp may be associated to the computer evidence constituted by the original documents, the related signature and the previous time-stamps. That operation shall be done prior to the expiry of the current time-stamp.

3. A valid time-stamp which has been associated to an electronic document as per ss (1) will guarantee the validity of the document even in the event the signature key is compromised but only provided the time-stamp was generated prior to the event in question.

Section 61 – Archiving of electronic documents

1. Electronic documents may be archived in accordance with the procedure established by AIPA Deliberation No. 24 of 30 July, 1998 and its modifications and integration even if they were created according to the provisions of Section 6(3) of the Presidential Decree 513/97.

2. The procedures established for documents originally created on electronic media under the provisions of Section 6(1)(b) of the Deliberation mentioned in ss (1) above shall be applicable to electronic documents.

3. The format restrictions as described in Section 6(1)(b) of the aforementioned Deliberation are not applicable to electronic documents. However, the person in charge of archiving may convert the electronic document into one of these formats while retaining in the archive the original document as the initial version of the archived document.

TITLE IV
Technical Rules applicable to Public Administration bodies

Section 62 – Certification by Public Administration bodies

1. In accordance with Section 17 of the Presidential Decree 513/97, Public Administration bodies independently supply with the certification of their public keys used during the administrative activity of their competence, observing the technical and security rules of previous sections. To such aim they may use the services offered by certification authorities included in the public list of Section 8 of the same Decree, respecting the norms related to public contracts.

2. The following dispositions continue to be applicable: Presidential Decree 522/97 with reference to the tasks about certification and temporal validation assigned to the “Technical Centre for assistance to bodies using the unitary network of the Public Administration” (“Centro Tecnico per la RUPA”) according to Section 15(2) of the law No. 59 of 15 March, 1997.

3. The following dispositions continue to be applicable: Decree of the Minister of Finance of 31 July, 1998, published in the Official Gazette No. 187 of 12 August, 1998, concerning the technical modalities for data transmission of the income-tax returns, and their modifications and integration.

TITLE V
Final provisions

Section 63 – Transitory norms

1. The above rules requiring checks following ITSEC evaluation levels are not to be applied during a 18 months period starting from the date when the application of this decree begins. Anyway, during that period, the supplier or the certification authority, according to its competence, must self-declare that the used devices comply with the security requirements specified by the above rules.