LAW no. 455 on July 18, 2001 on electronic signature

The Parliament of Romania adopts this law.

CHAPTER I: General Provisions

SECTION 1: General Principles

Art. 1.
This law regulates the legal status of the electronic signature and of the documents in electronic form as well as the requirements for electronic signatures certification service provision.

Art. 2.
This law shall be supplemented by the legal provisions on the conclusion, validity and effects of legal documents.

Art. 3.
No provision herein may be construed as constraining the parties' independent will and contractual freedom.

SECTION 2: Definitions

Art. 4. - For the purposes of this law:
1. Data in electronic form means information supplied in a conventional form appropriate for creating, processing, sending, receiving or storing that information by electronic means.
2. Document in electronic form means a collection of logically and operationally interrelated data in electronic form that reproduces letters, digits or any other meaningful characters in order to be read through software or any other similar technique.
3. Electronic signature means data in electronic form, which are included in, attached to or logically associated with a document in electronic form and serve as a method of identification.
4. Extended electronic signature means an electronic signature which meets all the conditions specified below:
a) it is uniquely linked to the subscriber;
b) it allows the identification of the subscriber;
c) it is created using means that the subscriber can maintain under his sole control;
d) it is linked to the data in electronic form to which it relates in such a manner that any subsequent change of that document is detectable.
5. Subscriber is a person who holds a signature-creation device and acts either on his own behalf or on behalf of a third party he or she represents.
6. Signature-creation data means unique data in electronic form, such as codes or private cryptographic keys, which are used by the subscriber to create an electronic signature.
7. Signature-creation device means configured software and/or hardware, used to implement the signature-creation data.
8. Secure-signature-creation device means a signature-creation device which meets all the requirements below:
a. the signature-creation data used for signature generation can practically occur only once

and their confidentiality can be ensured;
b. the signature-creation data used for signature generation cannot be derived;
c. the signature is protected from forgery by technological means currently available at the time it is generated;
d. the signature-creation data used for signature generation can reliably be protected by the subscriber against their unauthorized use;
e. it must not alter the data in electronic form to be signed or prevent these data from being presented to the subscriber prior to the completion of the signing process.
9. Signature-verification data means data in electronic form, including codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature.
10. Signature-verification device means configured software and/or hardware, used to implement the signature-verification data.
11. Certificate means a collection of data in electronic form that attests the link between a person and the signature-verification data, confirming the identity of that person.
12. Qualified certificate means a certificate that meets the requirements specified in Art. 18 and is issued by a certification service provider which complies with the provisions of Art. 20.
13. Certification service provider means a Romanian or foreign person that issues certificates or provides other electronic signature-related services.
14. Qualified-certification service provider is a certification service provider that issues qualified certificates.
15. Electronic signature related product means any software or hardware which are intended to be used by a certification service provider for the provision of electronic signature-related services or for the creation or verification of electronic signatures.

CHAPTER II: The Legal Status of the Documents in Electronic Form

Art. 5.
A document in electronic form that incorporates an electronic signature or has an electronic signature attached to or logically associated with it, based on a qualified certificate not suspended or not revoked at that time, and generated using a secure-signature-creation device is assimilated, in as much as its requirements and effects are concerned, to a document under private signature.

Art. 6.
A document in electronic form that includes an electronic signature or has an electronic signature attached to or logically associated with it, acknowledged by the party the respective document is opposed to, has the same effects as an authentic document, between those who signed it and between those who are representing their rights.

Art. 7.
Should the written form be required as proof or validity condition of a legal document in such cases as the law may provide, a document in electronic form shall satisfy to this condition if an extended electronic signature, based on a qualified certificate and created using a secure-signature-creation device was incorporated to, attached to or logically associated with it.

Art. 8.
(1) If either party does not recognize a document in electronic form or an electronic signature, the court will always direct that the verification shall be made by technical expertise.
(2) For this purpose, the expert or specialist shall require qualified certificates and any other documents necessary, according to the law, for the identification of the author of the document in electronic form, the subscriber or of the certificate owner.

Art. 9.
(1) The party that claims in court an extended electronic signature must prove that it meets the conditions provided for in Art. 4, item 4.
(2) The extended electronic signature based on a qualified certificate issued by an accredited certification service provider is presumed to satisfy the requirements of Art. 4, item 4.

Art. 10.
(1) The party claiming in court a qualified certificate must prove that the certification service provider which issued that certificate meets the conditions provided for in Art. 20.
(2) An accredited certification service provider is presumed to meet the conditions provided for in Art. 20.

Art. 11.
(1) The party that claims in court a secure-signature-creation device shall prove that the device meets the conditions provided for in Art. 4, item 8.
(2) A secure-signature-creation device that was homologated according to this law is presumed to meet the conditions provided for in Art. 4, item 8.

CHAPTER III: Certification Service Provision

SECTION 1: Common Provisions

Art. 12.
(1) Certification service provision is not subject to prior authorization and shall be performed in agreement with the principles of free and fair competition, and in compliance with the legal provisions in force.
(2) Certification service provision by service providers established in the Member States of the European Union shall be made under the requirements of the European Accord, establishing an association between Romania and the European Communities and their Member States.

Art. 13.
(1) Any person that contemplates providing certification services shall notify the supervisory and regulatory authority specialized in this field of the start-up of activity no later than 30 days before the date of commencement.
(2) Along with the notification provided in the 1st paragraph, certification service providers shall supply exhaustive information about the security and certification procedures they use and any further information the supervisory and regulatory authority specialized in this field may request.
(3) Certification service providers have the obligation to notify any intention of changing the security and certification procedures to the supervisory and regulatory authority specialized in

this field, with at least 10 days in advance, indicating the date and hour when the change enters into force, as well as the obligation to confirm in 24 hours the change effected.
(4) In emergency cases, where the security of certification services is affected, certification service providers can effect changes of the reported security and certification procedures and shall notify in 24 hours the supervisory and regulatory authority specialized in this field of the changes effected and of their justification.
(5) Throughout their activity, certification service providers shall observe their reported security and certification procedures notified according to 2nd, 3rd and 4th paragraphs above.

Art. 14.
(1) The certification service provider shall ensure access to any information necessary for the proper and safe use of its services. Such information shall be made available before entering into a contractual relation with the applicant for a certificate or on request from a third party that invokes a certificate.
(2) The information provided in the 1st paragraph shall be lodged in writing, in a readily accessible language and sent by electronic means, provided it can be stored and reproduced.
(3) The information provided in the 1st paragraph shall include at least:
a) the procedure to be followed for electronic signature creation and verification;
b) the tariffs charged;
c) the concrete ways and requirements for the use of certificates, including the limitations of their use, provided that such limitations are recognisable to third parties;
d) the obligations incurred by the certificate holder and certification service provider under this law;
e) reference to the accreditation, if applicable;
f) the contractual provisions under which the certificate was issued, including the limited liability of the certification service provider, if applicable;
g) modalities of dispute settlement;
h) any other information established by the supervisory and regulatory authority specialized in this field.
(4) The certification service provider shall send to the applicant a copy of the certificate.
(5) After the applicant has agreed to the certificate, the certification service provider shall enter the certificate in the register provided in Art. 17.

Art. 15.
(1) The natural persons that provide certification services in their own name and the personnel employed by a certification service provider, whether the latter is a natural or legal person, shall keep the secrecy of the information entrusted to them in their professional activity, except for such information the certificate holder may agree to be made public or to be communicated to third parties.
(2) The unauthorized breach of the obligation provided in 1st paragraph is tantamount to professional secrecy disclosure, which is an offence punishable under Art. 196 of the Criminal Code.
(3) Supplying information to a public authority when this authority acts in performance of its legal tasks and within the limits provided by law may not amount to professional secrecy disclosure.
(4) The obligation provided in the 1st paragraph shall apply also to the personnel of the supervisory and regulatory authority specialized in this field and to any person empowered by it.

Art. 16.
(1) The supervisory and regulatory authority specialized in this field and certification service providers are bound to comply with the legal provisions for processing of personal data.
(2) Certification service providers may collect personal data only from the applicant for a certificate, or, subject to the explicit agreement of the applicant, from third parties. Data may be collected to the extent they are required for certificate issuance and conservation. For any other purposes, data collection and use is subject to explicit agreement of the applicant.
(3) Whenever a pseudonym is used, the real identity of the holder may not be disclosed by the certification service provider unless the holder has agreed or except in such cases as provided at Art. 15, 3rd paragraph.

Art. 17.
(1) Certification service providers shall open and keep an electronic register of the certificates they issue.
(2) The electronic register of certificates shall specify:
a) the accurate date and time of issuance of a certificate;
b) the accurate date and time of expiry of a certificate;
c) the accurate date and time of suspension or revocation of a certificate, if applicable, including the causes thereof.
(3) The electronic register for record of certificates issued shall be available for consultation at any time, including on-line.

SECTION 2: Qualified Certification Service Provision

Art. 18.
(1) A qualified certificate shall contain the following mentions:
a) an indication that the certification was issued as a qualified certificate;
b) the identification data of the certification service provider as well as its citizenship if natural person, or nationality if legal person;
c) the name of the subscriber or a pseudonym, identified as such, and any other specific attributes thereof, provided they are relevant for the purpose for which the qualified certificate is intended;
d) the subscriber's personal identification code ;
e) the signature-verification data corresponding to the signature creation data under the exclusive control of the subscriber;
f) the period of validity of the qualified certificate;
g) the qualified certificate identification code;
h) the extended electronic signature of the certification service provider issuing the certificate;
i) constraints of the scope of the qualified certificate or limits on the value of transactions for which the certificate can be used, if applicable;
j) any other information established by the supervisory and regulatory authority specialized in this field.
(2) The certification service provider shall assign each subscriber a personal code for the purpose of uniquely identifying the subscriber.
(3) The generation of the personal identification code of the subscriber and the qualified certificate identification code shall be generated according to a methodology defined through regulations issued by the supervisory and regulatory authority specialized in this field.
(4) Further information other than required in the 1st paragraph may be supplied by a certification service provider in the certificate upon request of the holder, provided such

information is not contrary to the law, moral standards and public order, subject to prior checking for accuracy.
(5) The qualified certificate shall expressly indicate that a pseudonym is used, if the owner is identified by a pseudonym
.

Art. 19.

(1) Certification service providers shall check the identity of applicants on the exclusively basis of their identification papers before issuing them with qualified certificates.
(2) When issuing a qualified certificate, the certification service providers shall issue two copies of the certificate, on paper, out of which one is delivered to the holder and the other one shall be kept by the provider for no less than 10 years.

Art. 20.

To issue qualified certificates, certificate service providers must fulfill the following conditions:
a) shall have the financial, material, technological and human resources appropriate to guarantee the security, reliability and continuity of the certification services offered;
b) shall ensure the operation of a prompt and secure registration service to record the information provided in Art. 17, especially the prompt and secure operation of a suspension and revocation service for the qualified certificates;
c) shall ensure the possibility to accurately determine the date and time of issuance, suspension or revocation of a qualified certificate;
d) shall verify, by appropriate means and in accordance with the law, the identity and, if applicable, any specific attributes of the applicant for a qualified certificate;
e) shall employ personnel who possess the expert knowledge, experience and qualifications necessary for the provision of the above specified services, particularly competence at managerial level, expertise in electronic signature technology and enough practice in proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognized standards;
f) shall use electronic signature related products that are highly reliable, protected against modification and which ensure the technical and cryptographic security of the electronic signature certification process;
g) shall 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) shall keep all the information about a qualified certificate for at least 10 years after the validity of that certificate has expired, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings, should a dispute occur;
i) shall not store, reproduce or disclose to third parties the signature-creation data, except in such cases as the subscriber may require;
j) shall use reliable systems to store qualified certificates in a format that would meet the following requirements: only authorized persons can make entries and changes; the information may be checked for accuracy; qualified certificates may be consulted by third parties only if their holders have agreed; any technical change that may compromise these security requirements may be detected by authorized persons;
k) any other conditions established by the supervisory and regulatory authority specialized in this field.

Art. 21.
Qualified certification service providers must use only secure signature creation devices.

Art. 22.
(1) Qualified certification service providers shall have sufficient financial resources to cover the damage they may cause by their electronic signature certification-related activities.
(2) To ensure against such risks, they may subscribe an insurance policy issued by an insurance company or have a letter of guarantee issued by a specialty financial institution, or proceed in any other way established by decision of the supervisory and regulatory authority specialized in this field.
(3) The insured amount and the amount covered by the letter of guarantee shall be determined by the supervisory and regulatory authority specialized in this field.

SECTION 3: Suspension and Expiry of Certificates Validity

Art. 23.
(1) Any certification service provider shall suspend a certificate in 24 hours as of the moment it learns, or it should and could have learnt about one of the following situations:
a) subscriber's request, after checking his identity;
b) a court ruling so instructs;
c) the information contained in the certificate is no longer valid, if the revocation of the certificate is not mandatory;
d) any other circumstances that require suspension of the certificates under the security and certification procedures notified by the provider under Art. 13.
(2) Any certification service provider shall revoke a certificate in 24 hours from the moment it learns, or it should and could have learnt about one of the following situations:
a) subscriber’s request, after checking his identity;
b) the death of the subscriber or its interdiction;
c) an irrevocable court ruling so instructs;
d) should it be proved beyond reasonable doubt that the certificate was issued on the basis of faulty or fake information;
e) if the essential information contained in a certificate is no longer valid;
f) whenever the confidentiality of the signature-creation data has been violated;
g) a fraudulent use of a certificate;
h) any other circumstances that require revocation of the certificates under the security and certification procedures notified by the provider under Art. 13.
(3) The certification service provider shall forthwith notify the holder of the suspension or revocation of the certificate and give the reasons for such a decision.
(4) The certification service provider shall make an entry regarding the suspension or revocation decision in the electronic register provided at Art. 17, within 24 hours from the moment it learns, or it should and could have learnt that the decision to this effect is made.
(5) The suspension or revocation shall be opposable to third parties as soon as it is recorded in the electronic register.

Art. 24.
(1) Should a certification service provider plan to cease its electronic signatures certification-related activities or learn that it will no longer be able to provide them, it shall notify the supervisory and regulatory authority specialized in this field at least thirty days in advance of

its intention and about the appearance and nature of the circumstances that prevent it from continuing its activities.
(2) It is the duty of the certification service provider to notify the supervisory and regulatory authority specialized in this field, if it can no longer engage in electronic signatures certification-related activities and could not foresee this at least thirty days before actually halting operations, in 24 hours from the moment it learnt or it should and could have learnt about the circumstances preventing it from continuing its activities. The notice shall specify about the appearance and nature of the circumstances that make further operation impossible.
(3) A certification service provider may transfer all or part of its activities to another certification service provider subject to the following requirements:
a) the certification service provider shall notify every holder of valid certificates no less than thirty days in advance of its intention to transfer its electronic signatures certification-related activities to another certification service provider;
b) the certification service provider shall state the identity of the certification service provider it plans to transfer its activities to;
c) the certification service provider shall state to every certificate holder that the latter may choose not to accept the transfer, and set a time limit and the terms of refusal; should an explicit agreement of a certificate holder not be received within the time specified by the certification service provider, the latter shall revoke the certificate.
(4) Should any of the cases provided in paragraphs (1) and (2) be applicable to a certification service provider, and its activities not be taken over by another certificate service provider, it shall revoke the certificates within thirty days of notifying their holders and take appropriate action to ensure conservation of its archives and personal data processing in compliance with the law.
(5) For the purpose of this article, dissolution or liquidation, whether voluntary or judicial, bankruptcy and any other cases of cessation of operation, except for the enforcement of penalties provided by paragraphs (2) and (3) of Art. 33, shall be construed as cases of cessation of electronic signatures certification-related activities.

CHAPTER IV: Monitoring and Control

SECTION 1: Supervisory and regulatory authority

Art. 25.
The supervisory and regulatory authority specialized in this field has the responsibility for applying the provisions of this law and of the related regulations.

Art. 26.
(1) Within maximum 18 months from the publication of this law in the Official Gazette of Romania, a specialized public authority shall be established, with supervisory and regulatory tasks for the purposes of this law.
(2) Until the authority provided in the 1st paragraph is established, the supervisory and regulatory authority specialized in this field provided herein shall be the Ministry of Communication and Information Technology.

Art. 27.
The Ministry of Communication and Information Technology may delegate all or part of its responsibilities as supervisory and regulatory authority specialized in this field provided herein to another public authority in its coordination.

Art. 28.
(1) By the same time of the entry into force of this law, it shall be established the Certification Services Providers Register, hereinafter referred to as the Register, which is opened and updated by the supervisory and regulatory authority specialized in this field. The moment the specialized public authority provided in Art. 26 is established, the Register will be taken over and updated by this authority.
(2) The Register represents an official record:
a) of the certification services providers having headquarters in Romania;
b) of the certification services providers having the domicile or headquarters in another state and whose qualified certificates are recognized according to Art.40.
(3) The Register ensures, by making the records provided by this law, the storing of the identification data and of some information related to the activities of the certification service providers, as well as the public information regarding the data and information stored.
(4) The content and structure of the Register are established through regulations issued by the supervisory and regulatory authority specialized in this field.

Art. 29.
(1) The recording of the identification data and of the information related to the activities of the certification services providers mentioned in Art. 28, 2nd paragraph, in the Register provided in Art. 28, should be made on a personal application base, which must be submitted to the supervisory and regulatory authority specialized in this field no later than the date of commencement of provider's activity. (2) The mandatory content of the application and the necessary documentation will be established through regulations issued by the supervisory and regulatory authority specialized in this field.

Art. 30.
(1) The Register is public and permanently updated.
(2) The requirements for keeping the Register, for the access to the information which it contents, for the information that may be given to the applicant are established through regulations issued by the supervisory and regulatory authority specialized in this field.

SECTION 2: Supervision of Certification Service Providers business

Art. 31.
(1) The supervisory and regulatory authority specialized in this field may, ex officio or upon request of any interested person, check compliance of a certification service provider's activities with the provisions of this law or of the regulations issued on the basis thereof, or order that such compliance be checked.
(2) The control functions of the supervisory and regulatory authority specialized in this field as provided in the above paragraph shall be performed by purposefully empowered personnel.
(3) In order to perform their control functions, the control personnel is entitled to:
a) free, permanent access, according to the law, to any place where certification service provision equipment is located;
b) request any document or information that are necessary for control purposes;
c) check implementation of any security or certification procedure the certification service

provider being controlled may use;
d) seal off any equipment required for certification service provision or retain any document related to this kind of services for up to 15 days, if necessary;
e) take any other action provided by law.
(4) The control personnel shall:
a) not disclose the data they may learn in the exercise of their functions;
b) keep the sources of information relating to claims or intimations confidential.

Art. 32.
(1) Certification service providers are obliged to facilitate the exercise of control functions by the personnel such functions were entrusted to.
(2) In case of non-compliance with the obligation provided in 1st paragraph, apart from the penalty provided in Art. 44 letter c), the supervisory and regulatory authority specialized in this field may order the suspension of the activities of the certification service provider until the latter cooperates with the control personnel.

Art. 33.
(1) Should the control disclose non-compliance with the provisions of this law or of the regulations issued on the basis thereof, the supervisory and regulatory authority specialized in this field shall ask the certification service provider for compliance within such a time as it may set. During this time the supervisory and regulatory authority specialized in this field may order the suspension of the activity of the provider.
(2) Failure to comply within the time limit as provided in the above paragraph is a reason for the supervisory and regulatory authority specialized in this field to order the certification service provider to cease its activity and be erased from the Register.
(3) In the event of a serious breach of the legal provisions, the supervisory and regulatory authority specialized in this field may forthwith instruct that the respective certification service provider stop its activity and be struck off the Certification Service Providers' Register.

Art. 34.
(1) Whenever it orders a certification service provider to stop its activity, the supervisory and regulatory authority specialized in this field shall ensure either revocation of certificates of that certification service provider and of the subscribers, or that its activities or at least the electronic register of certificates issued and certificate revocation service are taken over by another certification service provider, subject to agreement by the latter.
(2) The supervisory and regulatory authority specialized in this field shall promptly notify the subscribers of the provider's end of activities and of the revocation of certificates or their take-over by another provider.
(3) Should no provider take over the activities of a certification service provider, the latter shall make sure that every certificate it may have issued is revoked. Should it fail to meet this obligation, the certificates shall be revoked by the supervisory and regulatory authority specialized in this field at the provider's expense.
(4) The supervisory and regulatory authority specialized in this field shall take over and keep the archives and the electronic register of certificates issued by the certification service provider whose activities were not taken over by another provider.

Art. 35.
(1) The striking off of the certification services providers shall be made on the base of the notification made to the supervisory and regulatory authority specialized in this field by the provider with at least thirty days before its cessation of activity.
(2) The striking off can be made also ex officio by the supervisory and regulatory authority specialized in this field, if it established by any means that the provider has ceased his activity.

SECTION 3: Voluntary Accreditation

Art. 36.
(1) In order to make proof of an increased level of security of the operations and of an appropriate level of protection of the lawful rights and interests of the users of certification services, certification service providers may apply to the supervisory and regulatory authority specialized in this field for accreditation.
(2) The conditions and the procedure for issuance, suspension and withdrawal of the accreditation decision, the content of such decision, as well as the effects of its suspension and withdrawal, shall be defined through regulations issued by the supervisory and regulatory authority specialized in this field, according to the principles of objectivity, transparency, direct proportionality and non-discriminatory treatment.
.
Art. 37.
(1) Certification service providers accredited according to this law are entitled to specify this status in every signature certification activity they may perform, in relation to the signatures certification.
(2) Certification service providers accredited according to this law shall ask that reference to this effect be made in the Register.

SECTION 4: Homologation

Art. 38.
(1) The secure-signature-creation devices shall be checked for compliance with this law by homologation agencies which may be public or private legal persons agreeable to the supervisory and regulatory authority specialized in this field in accordance with the conditions established through regulations issued by the latter.
(2) Upon completion of the checking procedure, a certificate of homologation of the secured signature-creation device is issued. The certificate may be withdrawn by the homologation agency should it find that the secured signature-creation device no longer complies with one of the provisions of this law.
(3) The conditions and procedure for the homologation agencies to be agreeable to the supervisory and regulatory authority specialized in this field shall be defined through regulations issued by the supervisory and regulatory authority specialized in this field.
(4) A decision of agreement shall be adopted by the supervisory and regulatory authority specialized in this field.

Art. 39.

(1) The supervisory and regulatory authority specialized in this field shall oversee compliance by the accreditation agencies of this law, of the regulations issued on the basis thereof and of the Decision of agreement.
(2) The provisions of Arts. 30-32 shall apply mutatis mutandis to the supervisory and regulatory authority specialized in this field's control over the activities of the homologation agencies.

CHAPTER V: Acknowledgment of Certificates Issued by Foreign Certification Services Providers

Art. 40.
A qualified certificate issued by a certification service provider having its domicile or headquarters in another country shall be acknowledged as having the same legal effects as a qualified certificate issued by a certification service provider residing or having its domicile or headquarters in Romania if:
a) the certification service provider having its domicile or headquarters in another country was accredited according to this law; or
b) an accredited certification service provider having its domicile or headquarters in Romania guarantees the certificate; or
c) the certificate or the certification service provider that issued it is recognized by virtue of a bilateral or multilateral agreement between Romania and other states or international organizations on a mutual basis.

CHAPTER VI: Liability of Certification Service Providers

Art. 41.
A certification service provider that issues certificates presented as being qualified or guarantees such certificates is liable for damage caused to any person the behavior of which is based on the legal effects of such certificates concerning:
a) the accuracy at the time of issuance of a certificate of all the information included therein;
b) the assurance that, at the time of issuance of a certificate, the subscriber identified in the certificate held the signature-creation data corresponding to the signature-verification data referred to in the respective certificate;
c) the assurance that the signature-creation data were consistent with the signature-verification data, if the certification service provider generates them both;
d) the suspension and revocation of the certificate, in cases and conditions provided in Art. 24 1st and 2nd paragraphs;
e) the fulfillment of and and all obligations provided by Arts. 13-17 and 19-22 herein,
unless the certification service provider proves that, in spite of his due diligence, he could not prevent the damage from occurring.

Art. 42.
(1) A certification service provider may indicate the qualified certificate limitations of the scope of use of the certificate or limits on the value of transactions for which the certificate can be used, provided that the limitations or limits are recognizable to third parties.
(2) A certification service provider may not be held liable for damage arising from the use of a qualified certificate in breach of the limitations or limits provided therein.

CHAPTER VII: Obligations of Certificate Holders

Art. 43.
Certificate holders shall promptly apply for revocation of their certificates if:
a) they lost the signature-creation data;
b) have reasons to believe the signature-creation data are known to an unauthorized third party;
c) the essential information contained in the certificate is no longer valid.

CHAPTER VIII: Administrative Violations and Penalties

Art. 44.
There shall be contravention if, according to law is not an offence, and punishable by fines ranging from ROL 5,000,000 to ROL 100,000,000 the certification services provider's deed related to the:
a. failure to send the notice provided at Art. 13 paragraph (1);
b. failure to notify the supervisory and regulatory authority specialized in this field of the security and certification procedures used in such conditions and within such time as provided at Art. 13;
c. non-compliance with the obligation to facilitate the exercise of control functions by the supervisory and regulatory authority specialized in this field's duly empowered personnel;
d. transfer of electronic signatures certification activities in breach of the provisions of Art. 24 paragraph (3).

Art. 45.
There shall be contravention if, according to law is not an offence, and punishable by fines ranging from ROL 10,000,000 to ROL 250,000,000 the certification services provider's deed related to the:
a. failure to provide the persons specified in Art. 14, 1st paragraph, in compliance with the conditions provided in Art. 14, 1st and 2nd paragraphs, and with the mandatory information provided in Art. 14, 3rd paragraph, or to provide all this information, as well as to provide accurate information;
b. non-compliance with the obligation concerning the processing of personal data provided in Art. 16;
c. failure to make the entries required by law in the electronic register provided in Art. 17, or to make them within the time limit required by Art. 14, 5th paragraph, Art. 23, 1st or 2nd paragraph, or to make them accurately;
d. issuance of certificates presented as qualified to applicants, when such certificates do not contain all the mandatory specifications required by Art. 18;
e. issuance of qualified certificates containing information that is inaccurate, or contrary to the law, morals or public order, or that was not checked for accuracy as provided by Art. 18, 4th paragraph;
f. issuance of qualified certificates without the applicant's identity being checked, as Art. 19 provides; g. failure to take action that would guarantee confidentiality in the process of signature data generation, should the provider generate such data;
h. failure to keep all the information about a qualified certificate for at least 5 years after the

validity of the certificate has expired;
i. storage, reproduction or disclosure of signature-creation data to third parties, unless the subscriber so requires, in cases where the provider issues qualified certificates;
j. storage of qualified certificates in a format that is in breach of the provisions of art. 20, letter j);
k. use of signature-creation devices in violation of the provisions of Art. 4, 8th paragraph herein, in cases where the provider issues qualified certificates;
l. if the provider intends to end its activities, or in any of the cases provided in Art. 24, 5th paragraph, when impossible for the provider to continue the activity, failure to notify the supervisory and regulatory authority specialized in this field at least thirty days in advance of the specific circumstances that make further operation impossible or of its intention;
m. in any of the cases provided in Art. 24, 5th paragraph, if impossible for the provider to continue the activity and the provider could not foresee this situation with at least thirty days in advance, failure to notify within the term provided in Art. 24, 2nd paragraph of the specific circumstances that made it impossible for the continuation of electronic signatures certification-related activities;
n. failure to take appropriate action, in any of the cases provided at Art. 24, 1st and 2nd paragraphs, to ensure conservation of the archives or processing of personal data so as the law provides;
o. failure to suspend or to revoke the issued certificates, when suspension or revocation is compulsory, or failure to do so within the time provided by law;
p. continuation of electronic signatures certification activities when the supervisory and regulatory authority specialized in this field instructed that such activities be suspended or ended;
q. undue use of the accredited provider status through a specific reference to that effect or in any other way in the issuance of certificates or performance of other electronic signatures certification-related activities;
r. failure to apply for registration of the data and information provided in Art.29. at the Certification Service Provider's Register, within the term provided in Art. 29, 1st paragraph.

Art. 46.
Non-compliance by the homologation agency of its obligation to facilitate the exercise of control functions by duly delegated supervisory and regulatory authority specialized in this field's personnel is an administrative violation punishable by fines ranging from ROL 15,000,000 to ROL 250,000,000.

Art. 47. The assertion of the contraventions and the application of the penalties provided for herein shall be enforced by the supervisory and regulatory authority specialized in this field's personnel entrusted with control functions.

Art. 48. The provisions of this Chapter shall be complemented by the provisions of Law No.32/1968 on ascertaining and sanctioning contraventions.

CHAPTER IX: Final provisions

Art. 49.
(1) The level of tariffs established by the homologation agencies for the homologation of secure-signature-creation devices and for the additional services shall be freely established, in

compliance with the Competition Law no. 21/1996.
(2) The agencies mentioned in 1st paragraph may gather tariff with different rates for different geographical areas or for emergency services, for on-line registrations or through the Internet, respecting their own commercial strategies and the legal provisions.
(3) Shall be forbidden for the agencies or their representatives to publish comparative tables, regarding the tariffs rating, and to adopt any measures that may restrict the commercials regarding the tariffs rating charged by the agencies for providing their services.

Art. 50.
(1) The activities of the homologation agencies are subject to the provisions of the Competition Law No. 21/1996, regarding the establishment of the fees rating for the services provided and regarding the acts or facts that can restrict in any way the competition on the above mentioned services market.
(2) The homologation agencies are also subject to the provisions of the Law no. 11/1991 considering any of its meanwhile modifications, regarding the unfair competition.

Art. 51.
The amount of the penalties provided in the low herein will be updated by Government Decision taking account of the evolution of the inflation rate.

Art. 52.
Within a three months period from the publication of this law in the Official Gazette of Romania 1st part, the supervisory and regulatory authority specialized in this field shall elaborate the Rules of enforcement of this law.

Art. 53.
This law enters into force at the date of its publication in the Official Gazette of Romania, 1st part and will be enforced after 3 months as of its entry into force.

This law was adopted by the Senate in the session from June 26, 2001, subject to the observance of the provisions of Art. 74, paragraph (1), from the Constitution of Romania.

p. PRESIDENT OF THE SENATE
DORU IOAN TARACILA

This law was adopted by the Chamber of Deputies in the session from June 28, 2001, subject to the observance of the provisions of Art. 74 par. (1) from the Constitution of Romania.

PRESIDENT OF THE CHAMBER OF DEPUTIES
VALER DORNEANU

Published in the Official Gazette no. 429 of July 31, 2001