LAW FOR THE ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE

Prom. SG. 34/6 Apr 2001, amend. SG. 112/29 Dec 2001, amend. SG. 30/11 Apr 2006, amend. SG. 34/25 Apr 2006, amend. SG. 38/11 May 2007

Chapter one.
GENERAL

Field of application
Art. 1. (1) This law determines the electronic document, the electronic signature and the conditions and the order of providing certifying services.
(2) This law shall not apply:
1. regarding transactions for which the law requires qualified written form;
2. when the holding of the document or a copy of it has legal importance (securities, bills of lading, etc.).

Chapter two.
ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE

Electronic statement
Art. 2. (1) Electronic statement is a verbal statement presented in digital form by a generally adopted standard of transformation, reading and visual presentation of the information.
(2) The electronic statement can also contain non-verbal information.

Electronic document
Art. 3. (1) Electronic document is an electronic statement written on a magnetic, optic or other carrier enabling reproduction.
(2) The written form shall be considered complied with if an electronic document is compiled.

Author and titular of the electronic statement
Art. 4. Author of the electronic statement is the individual indicated in the statement as its author. Titular of the electronic statement is the person on whose behalf the electronic statement is made.

Addressee of the electronic statement
Art. 5. The addressee of the electronic statement can be a person who, by virtue of a law, is obliged to receive electronic statements or which, on the grounds of unambiguous circumstances, can be considered agreed to receive the statement in electronic form.

Mediator of the electronic statement
Art. 6. (1) Mediator of the electronic statement is a person who, by assignment of the titular, sends, receives, records or stores an electronic statement or performs other services related to it.
(2) The mediator of the electronic statement shall be obliged:
1. to have technical and technological equipment which provides reliability of the used systems;
2. to keep personnel possessing the necessary expert knowledge, experience and qualification;
3. to provide conditions for precise determination of the time and source of the transmitted electronic statements;
4. to use reliable systems for storing the information under item 3;
5. (amend., SG 38/07) to store the information under item 3 for a period of two years.
(3) The mediator of the electronic statement shall be responsible for the caused damages by non-fulfilment of his obligations under para 2.

Mistake in transmitting electronic statement
Art. 7. The titular shall bear the risk of mistakes in transmitting electronic statement, unless the addressee has not taken due care.

Receiving the electronic statement
Art. 8. (1) The electronic statement shall be considered received if the addressee confirms the receipt.
(2) If a term of confirmation of the receipt is not stipulated the confirmation must be made within reasonable period.
(3) The confirmation of the receipt shall not certify the contents of the electronic statement.

Time of sending the electronic statement
Art. 9. The electronic statement shall be considered sent with its receipt in an information system which is not controlled by the author.

Time of receiving the electronic statement
Art. 10. (1) The electronic statement shall be considered received with the sending of confirmation by the addressee of its receipt.
(2) If confirmation is not required the electronic statement shall be considered received with its receipt in the information system indicated by the addressee. If the addressee has not indicated an information system the statement shall be considered received with its receipt in the information system of the addressee, and if the addressee has no information system - with its drawing out by the addressee of the information system where the statement has been received.

Time of learning about the electronic statement
Art. 11. It shall be considered that the addressee of the electronic statement has learned about its contents within a reasonable period after its receipt.

Place of sending and receiving the electronic statement
Art. 12. (1) The electronic statement shall be considered sent from the place of activity of its titular.
(2) The electronic statement shall be considered received at the place of activity of its addressee.
(3) If the titular or the addressee of the statement has more than one place of activity considered as place of activity shall be the one which is most closely related to the statement and its fulfilment, taking into account the circumstances which have been known to the titular and to the addressee or have been taken into consideration by them at any time before or during the performance of the statement.
(4) If the titular or the addressee has no place of activity his permanent residence shall be taken into consideration.

Electronic signature
Art. 13. (1) Electronic signature is:
1. every information related to the electronic statement in a way coordinated between the author and the addressee, secure enough with respect of the exchange which:
a) discloses the identity of the author;
b) discloses the consent of the author with the electronic statement, and
c) protects the contents of the electronic statement against subsequent changes;
2. the transformed electronic signature;
3. the universal electronic signature.
(2) The electronic signature under item 1 and 2 has the validity of a sign manual unless a titular or addressee of the electronic statement is a state body or a body of the local independent government.
(3) The universal electronic signature has the validity of a sign manual regarding everybody. The Council of Ministers shall determine the state bodies which can use in their relations another type of electronic signature.

Confidentiality of the data for creation of the electronic signature
Art. 14. Nobody, besides the author, shall have the right to access to the data for creation of the electronic signature.

Contesting the electronic signature
Art. 15. (1) The person defined as titular or author of the electronic statement cannot contest the authorship regarding the addressee if the statement is signed by an electronic signature when:
1. the statement is sent through an information system operating in automatic regime, or
2. the statement has been made by a person having access to the way of identification.
(2) Para 1, item 2 shall not apply from the moment when the addressee receives notification that the electronic statement does not originate from the author and the addressee has sufficient time to comply his conduct with the notification.
(3) Para 1 shall not apply when the addressee of the statement has not taken the due care.

Chapter three.
TRANSFORMED ELECTRONIC SIGNATURE

Section I.
General

Definition
Art. 16. (1) Transformed electronic signature is a transformed electronic statement, included, added or logically related to the same electronic statement before the transformation.
(2) The transformation under para 1 shall be carried out through algorithms including the using of the private key-word of asymmetric cryptographic system.
(3) The requirements for the algorithms shall be determined by an ordinance of the Council of Ministers.

Mechanism of creation and verification of transformed electronic signature
Art. 17. (1) The persons creating transformed electronic signature must apply a mechanism guaranteeing that:
1. the data used for the creation of the electronic signature can be reproduced only by its creation and their security is duly protected;
2. the data used for creation of the electronic signature are not accessible, cannot be drawn out and the signature is protected against forgery;
3. the data for creation of the electronic signature can be protected by the author against their using by other persons;
4. the contents of the statement shall be accessible to the author and shall remain unchanged until the creation of the electronic signature.
(2) The persons who carry out verification of a transformed electronic signature must apply a mechanism guaranteeing that:
1. the data for establishing the using of the private key-word correspond to the data submitted to the person using the public key-word;
2. the using of the private key-word has been reliably verified and the results from this verification have been submitted to the person who had used the public key-word.

Confidentiality of the private key-word
Art. 18. Nobody besides the author shall have the right to access to the private key-word.

Section II.
Providers of identification services

Activity of the providers of identification services
Art. 19. (1) Provider of identification services is a person who:
1. issues certificates according to art. 24 and keep registers for them;
2. provides to every third person access to the published certificates.
(2) The provider of identification services can provide services for creation of private and public key-word for transformed electronic signature.

Organisations for voluntary accreditation
Art. 20. (1) Providers of identification services can establish organisations for voluntary accreditation with the purpose of achieving higher level of the identification services provided by them.
(2) The organisations for voluntary accreditation shall assist the acknowledgement of the legal status of the certificates issued by Bulgarian providers abroad, as well as of certificates issued by foreign providers in the Republic of Bulgaria.
(3) The conditions for participation in an organisation for voluntary accreditation must be generally accessible and must create equality of all providers of identification services.

Requirements for the activity of the providers of identification services
Art. 21. (1) The providers of identification services shall carry out their activity by:
1. maintaining available resources which enable the fulfilment of the activities in compliance with the requirements of this law;
2. insuring themselves for the time of their activity against damages caused by non-fulfilment of their obligations under this law;
3. having technical equipment and technologies which provide reliability of the used systems, as well as technical and cryptographic security of the processes performed by them;
4. maintaining personnel having the necessary expert knowledge, experience and qualification for carrying out the activity, more specifically in the sphere of the technology of the transformed electronic signatures, as well as good knowledge of the security procedures.
5. providing conditions for precise definition of the time of issuance, suspension, renewal and termination of the validity of the certificates;
6. providing measures against forging the certificates and the confidentiality of the data to which they have access in the process of creation of the signature;
7. using reliable systems for storing and management of the certificates which ensure that:
a) only duly authorised employee have access for introduction of changes;
b) establishment of the authenticity and validity of the certificates;
c) possibility of limited access to the published certificates;
d) the occurrence of technical problems in connection with the security become immediately known to the servicing personnel;
e) with the expiration of the validity of the certificate the possibility of confirmation of the private key-word is terminated;
8. providing possibility of immediate stopping and termination of the validity of the certificates;
9. (Amend. SG 112/01) informing immediately the Commission for regulation of the communications about the starting of activity according to art. 19.
(2) The Council of Ministers shall adopt ordinance under para 1, item 1, 2 and 3.
(3) The provider of identification services cannot use the information stored by him for purposes different from those related to his activity. He can submit to third persons only the information contained in the certificates.

Obligations of the provider of identification services
Art. 22. The provider of identification services shall be obliged:
1. to issue certificate upon request of every person informing him in advance whether he is registered by the order of chapter fur and about his participation in organisations for voluntary accreditation;

2. to inform the persons requesting the issuance of certificates about the conditions of issuance and using the certificate, including about the restrictions of its validity, as well as about the procedures of filing complaints and settlement of disputes;
3. when issuing certificates to verify through the admissible means the personality, respectively the identity, of the author and of the titular of the transformed electronic signature and, where necessary - other data regarding these persons, included in the certificate;
4. to publish the issued certificate so that third persons can have access to it according to the instructions of the titular;
5. not to store or copy data for creation of private key-words;
6. to undertake immediate activities in connection with the stopping, renewal and termination of the validity of the certificate upon establishing the respective grounds for that;
7. to inform immediately the author and the titular about circumstances regarding the validity or reliability of the issued certificate;
8. to possess a transformed electronic signature which shall be used only in connection with his activity as provider of identification services.

Relations with the titular
Art. 23. The relations between the provider of identification services and the titular shall be settled by a written contract.

Section III.
Certificates for transformed electronic signature

Certificate
Art. 24. (1) The certificate is an electronic document, issued and signed by the provider of identification services containing:
1. (amend. - SG 34/06, in force from 01.10.2006) the name, the address, the unified citizens code or the unified identification code of the provider of identification services, as well as indication of his nationality;
2. (amend. - SG 34/06, in force from 01.10.2006) the name or the company, the address, data for the registration of the titular of the transformed electronic signature;
3. grounds for the authorisation, the name and address of the individual (the author) authorised to make electronic statements on behalf of the titular of the transformed electronic signature;
4. the public key-word corresponding to the private key-word of the titular of the transformed electronic signature;
5. the identifiers of the algorithms by which are used the public key-words of the titular of the transformed electronic signature and of the provider of identification services;
6. the date and the hour of issuance, suspension, renewal and termination of the validity;
7. term of validity;
8. the limitations of the validity of the signature;
9. the unique identification code of the certificate;
10. the responsibility and the guarantees of the provider of identification services;
11. (Amend. SG 112/01) reference to the certificate for the transformed electronic signature under art. 22, item 8 of the provider of identification services, as well as to the registration of the provider in the Commission for regulation of the communications.
(2) When the authorisation of the author originates from other authorised persons the certificate must contain data under para 1, item 2 for these persons.
(3) Unless otherwise agreed the certificate shall be valid for a period of three years.
(4) The titular and the author shall be obliged to inform immediately the provider of identification services about occurred changes of the circumstances indicated in the certificate.
(5) The changes of the circumstances indicated in the certificate cannot be set against third conscientious persons.

Issuance of certificate

Art. 25. (1) The provider of identification services shall issue certificate upon written request of the titular.
(2) The request under para 1 shall be granted if:
1. it originates from the titular or from a person duly authorised by him;
2. the information regarding the titular, presented for inclusion in the certificate, is correct and full, and
3. the private key-word:
a) is held by the titular;
b) is technically fit to be used for creation of a transformed electronic signature, and
c) corresponds to the public key-word, so that it can be certified through the public key-word that a definite transformed electronic signature is created by the private key-word.
(3) If the requested certificate regards a transformed electronic signature with an author different from the titular the request shall be granted if the requirements under para 2 are met and:
1. the information regarding the author submitted for inclusion in the certificate is also correct and full, and
2. the private key-word is held by the author.
(4) When the request is granted the provider of identification services shall require from the titular, respectively the author, to accept the contents of the requested certificate. He shall change the contents of the certificate if the titular, respectively the author, points out incorrectness or incompleteness.
(5) The provider of identification services shall issue immediately the certificate whose contents have been accepted by the order of para 4 by publishing it in the register for the certificates.

Suspension and renewal of the validity of the certificate
Art. 26. (1) Unless it is agreed otherwise the provider of identification services shall have the right to suspend the validity of the certificate issued by him for a period required by the circumstances, but for no longer than 48 hours, if a grounded doubt exists that the validity of the certificate must be terminated.
(2) Unless it is agreed otherwise the provider of identification services shall be obliged to suspend the validity of a certificate issued by him for a period required by the circumstances but for no longer than 48 hours:
1. upon request of the titular, respectively the author, without being obliged to establish the identity or the power of representation;
2. upon request of a person for whom, according to the circumstances, it is obvious that he might be aware about the security of the private key-word as a representative, partner, employee, member of the family, etc.;
3. (Amend. SG 112/01) upon request of the Commission for regulation of the communications.
(3) (Amend. SG 112/01) In the presence of an immediate danger for the interests of third persons or in the presence of enough information for violation of the law the Chairman of the Commission for regulation of the communications can oblige the respective provider of identification services to suspend the validity of the certificate for a period required by the circumstances, but for no longer than 48 hours.
(4) The provider of identification services shall immediately inform the titular and the author about the suspension of the validity of the certificate.
(5) The suspension of the validity of the certificate shall be carried out by creating impossibility of access to it.
(6) The validity of the certificate shall be renewed by:
1. the expiration of the term of suspension;
2. (Amend. SG 112/01) by the provider of identification services - upon dropping the grounds for suspension or upon request of the titular, after the provider of identification services, respectively the Commission for regulation of the communications, assure themselves that he has learned about the reason of the suspension, as well as that the request for renewal has been made as a result of the learning.

Termination of the validity of the certificate
Art. 27. (1) The validity of the certificate shall be terminated:
1. upon expiration of the term;
2. upon death or placing under judicial disability of the individual - provider of identification services;

3. upon termination of the corporate body of the provider of identification services without transferring the activity to another provider of identification services.
(2) The provider of identification services shall be obliged to terminate the validity of the certificate upon request of the titular or the author upon verification of the identity and the representative authority of the titular, respectively the author.
(3) The supplier of identification services shall terminate the validity of he certificate upon:
1. death or placing under judicial disability of the titular or the author;
2. termination of the corporate body of the titular;
3. termination of the representative authority of the author regarding the titular;
4. establishing that the certificate has been issued on the grounds of false data.

Register of the certificates
Art. 28. (1) The provider of identification services shall keep an electronic register where he shall publish the certificate for his electronic signature according to art. 22, item 8 and the issued certificates.
(2) The provider of identification services cannot restrict the access to the register. Only the author can restrict the access to the certificate for his signature.
(3) The provider of identification services shall publish in the register under para 1 information for:
1. the conditions and the order of issuing certificate, including for the rules of establishing the identity of the titular of the transformed electronic signature;
2. the security procedures of the provider of identification services;
3. the way of using the transformed electronic signature;
4. the conditions and the order of using the transformed electronic signature, including the requirements for storing the private key-word;
5. the conditions of access to the certificate and the way of verification of the transformed electronic signature;
6. the price of obtaining and using certificate, as well as the prices of the remaining services submitted by the provider of identification services;
7. the responsibility of the provider of identification services and of the titular of the transformed electronic signature;
8. the conditions and the order by which the titular extends request for termination of the validity of the transformed electronic signature.
(4) The order of keeping the register under para 1 shall be settled by an ordinance of the Council of Ministers.

Section IV.
Responsibility

Responsibility of the provider of identification services
Art. 29. (1) The provider of identification services shall be responsible to the titular of the transformed electronic signature and to every third persons for the damages:
1. caused by non-fulfilment of the requirements of art. 21 and of the obligations under art. 22 and 25;
2. from false or missing data in the certificate by the moment of its issuance;
3. he causes in case that during the issuance of the certificate the person, indicated as an author, has not possessed the private key-word corresponding to the public key-word;
4. caused by non-compliance between the data for verifying the using of the private key-word and the data submitted to the person using the public key-word.
(2) Invalid is the agreement excluding or restricting the responsibility of the provider of identification services for negligence.
(3) The provider of identification services shall not be liable for damages caused by using the certificate out of the scope of the restrictions of its validity included in it.

Responsibility of the titular and of the author to third persons
Art. 30. (1) The titular shall be responsible to third conscientious persons when, during the creation of the pair of public and private key-word algorithm has been used which does not meet the requirements of the ordinance under art. 16, para 3.

(2) The titular shall be responsible to the third conscientious persons if the author:
1. does not meet precisely the security requirements determined by the provider of identification services;
2. does not request from the provider of identification services termination of the validity of the certificate upon learning that the private key-word has been used without authorisation or there is a danger of its unauthorised using.
(3) The titular who has accepted the certificate upon its issuance shall be responsible to the third conscientious persons:
1. if the author is not authorised to keep the private key-word corresponding to the public key-word indicated in the certificate;
2. for false statements made before the provider of identification services and related to the contents of the certificate.
(4) The author who has accepted the certificate upon its issuance shall be responsible to third conscientious persons if he has not been authorised to request the issuance of the certificate.

Responsibility of the titular and of the author to the provider of identification services
Art. 31. The titular, respectively the author, shall be responsible to the provider of identification services if he has accepted the certificate issued by the provider of identification services on the grounds of false data submitted by him, respectively on the grounds of data concealed by him.

Section V.
Regulation and control

Powers of the Commission for regulation of the communications (Title amend. SG 112/01)
Art. 32. (1) (Amend. SG 112/01) The Commission for regulation of the communications shall have the following powers:
1. exercise control of the providers of identification services regarding the reliability and security of the identification services;
2. approve the manuals for the consumers and the prescribed security procedures;
3. work out, coordinate and propose for adoption by the Council of Ministers draft ordinance according to this law.
(2) (Amend. SG 112/01) In fulfillment of its functions the Commission for regulation of the communications shall have the right:
1. to free access to the sites subject to control;
2. to inspect the documents for qualification of the employees of the providers of identification services;
3. to require references and documents related to the exercising of the control;
4. to appoint persons who shall carry out inspection of the observance by the providers of identification services of the requirements under art. 17 and art. 21, para 1.
(3) (Amend. SG 112/01) The Commission for regulation of the communications shall maintain and publish a list of the persons under para 2, item 4.
(4) The activity of the providers of identification services and the order of termination of their activity, the requirements regarding the form of the certificates issued by the providers of identification services, the requirements for storing the information regarding the services submitted by the providers of identification services, the requirements for the contents, the form and the sources in connection with the disclosed information by the providers of identification services, the requirements for the persons under para 2, item 4, as well as the conditions and the order of their inclusion in the list under para 3 shall be determined by an ordinance of the Council of Ministers.

Chapter four.
UNIVERSAL ELECTRONIC SIGNATURE

Definition
Art. 33. (1) Universal electronic signature is the transformed electronic signature whose certificate is issued by the provider of identification services, registered according to art 34.
(2) Universal are also:
1. (Amend. SG 112/01) the electronic signature of the Commission for regulation of the communications by which it signs the acts issued on the grounds of its powers by law;
2. the electronic signatures under art. 22, item 8 of the registered providers of identification services.

Register institution
Art. 34. (Amend. SG 112/01) (1) The Commission for regulation of the communications shall register providers of identification services and shall keep register of the certificates for their transformed electronic signatures according to art. 22, item 8.
(2) The Commission for regulation of the communications shall publish in the register under para 1 the certificate for its electronic signature according to art. 33, para 2, item 1.

Powers of the Commission for regulation of the communications regarding the registered providers (Title amend. SG 112/01)
Art. 35. (1) (Amend. SG 112/01) The Commission for regulation of the communications shall have the following powers:
1. register the providers of identification services;
2. refuse registration of providers of identification services when they do not meet the necessary requirements;
3. delete the registration of the providers of identification services.
(2) (Amend. SG 112/01) The Commission for regulation of the communications shall issue references for the public key-words of the registered providers of identification services. The reference shall be electronic, shall contain the certificates and shall be signed by the universal electronic signature of the Commission for regulation of the communications.

Registration of the providers of identification services
Art. 36. (1) In filing application for registration as provider of identification services the applicant shall present:
1. (amend. - SG 34/06, in force from 01.10.2006) current certificate of registration in the commercial register;
2. insurance policy according to art. 21, para 1, item 2;
3. the rules for issuance of certificates, including the rules for establishing the identity of the titular of the universal electronic signature;
4. the security procedures applied in issuing and using the universal electronic signature;
5. the conditions and the order of using the universal electronic signature, including the requirements for storing the private key-word;
6. the price of receiving and using certificates, as well as the prices of the remaining services submitted by the provider of identification services;
7. declaration stating that the requirements under art. 21, para 1, item 1, 3 and 4 have been met;
8. documents proving the fulfillment of the requirements under art. 17 and art. 21, para 1, item 5 - 8.
(2) The application for registration shall be considered within one month. Registration can be refused only if the applicant has not presented the necessary documents, does not meet the requirements of art. 21, para 1 and art. 17 or has not paid the necessary state fee.
(3) The notification for the refusal must state all shortcomings of the application.
(4) (amend. - SG 30/06, in force from 12.07.2006) The refusal for registration shall be appealed by the order of the Administrative procedure code.
(5) The applicant can remove the shortcoming and file a new application.
(6) The order of registration shall be determined by an ordinance of the Council of Ministers.

Deletion of the registration
Art. 37. (1) The registration shall be deleted:
1. in case the applicant presents false data;
2. for gross or systematic violation of this law and of the by-law normative acts for its implementation.
(2) The activity of the registered provider of identification services shall be terminated by the deletion of the registration unless the activity is transferred to another registered provider of identification services.
(3) The termination of the activity of a registered provider of identification services related to issuance of certificates for universal electronic signatures shall be settled by an ordinance under art. 32, para 4.

Register of the providers of identification services
Art. 38. (1) The Register of the providers of identification services shall be public. Everybody can request reference for the registered providers of identification services.
(2) Everybody can request reference for the conditions and the order of registration of the provider of identification services.

State fees
Art. 39. (1) For registration of the providers of identification services and for the issuance of references under art. 35, para 2 shall be collected state fee.
(2) The size of the state fee shall be determined by a tariff approved by the Council of Ministers.

Activity of the registered provider of identification services
Art. 40. The registered provider of identification services who has issued certificate for universal electronic signature shall certify the date and the hour of submitting an electronic documents signed by him.

Chapter five.
APPLICATION OF THE ELECTRONIC DOCUMENT AND OF THE UNIVERSAL ELECTRONIC SIGNATURE BY THE STATE AND THE MUNICIPALITIES

Obligation for acceptance and issuance of electronic documents
Art. 41. (1) The Council of Ministers shall determine its bodies which:
1. cannot refuse the acceptance of electronic documents signed by a universal electronic signature;
2. cannot refuse the issuance in the format of electronic document, signed by a universal electronic signature, permits, licenses, approvals and other administrative acts.
(2) The acceptance and the issuance of electronic documents signed by universal electronic signature in the judiciary system shall be settled by a law.
(3) The acceptance and the issuance of electronic documents signed by universal electronic signature by other state bodies, other than those under para 1 and 2, and by the bodies of the local independent government shall be settled by their acts. The order and the format of working out and storing the electronic documents shall be settled by internal rules.

Storing electronic documents
Art. 42. The state bodies and the bodies of the local independent government shall be obliged to store the electronic documents within the normative terms for storing documents.

Chapter six.
PROTECTION OF THE PERSONAL DATA

Obligations for protection of the personal data
Art. 43. (1) The protection of the personal data gathered by the providers of identification services for the needs of the activity carried out by them, and the protection of the kept registers shall be settled by a law.
(2) (Amend. SG 112/01) The regime under para 1 shall also apply regarding the personal data announced to the Commission for regulation of the communications which, in fulfillment of its obligations shall monitor the activity of the providers of identification services.
(3) The providers of identification services shall gather personal data for the author and for the titular of the signature only inasmuch as they are necessary for the issuance and using of a certificate.
(4) Data for a third person can be gathered only by the explicit consent of the person whom they regard.
(5) The gathered data cannot be used for purposes other than those under para 3, except by the explicit consent of the person whom they regard, or if it is allowed by a law.

Chapter seven.
RECOGNITION OF CERTIFICATES ISSUED BY PROVIDERS OF IDENTIFICATION SERVICES ESTABLISHED IN OTHER COUNTRIES

Grounds and order
Art. 44. (1) Certificates issued by providers of identification services, established in other countries according to the national legislation of these countries, shall be recognised as equal to certificates issued by a Bulgarian provider of identification services if some of the following conditions is fulfilled:
1. the obligations of the provider of identification services who has issued the certificate, and the requirements for his activity shall meet the requirements stipulated by this law and the provider of identification services is recognised in the country where he is established;
2. a Bulgarian provider of identification services accredited by an organisation under art. 20 or is registered according to art. 34 shall be responsible for the activities and inactivity of a provider of identification services established in another country in the cases under art. 29, or
3. the certificate or the provider of identification services who has issued the certificate is recognised by an enacted international agreement.
(2) (Amend. SG 112/01) The conditions under para 1, item 1 and 2 shall be specified by the Commission for regulation of the communications by the publishing in an electronic register of:
1. the certificates for the public key-words of the foreign providers of identifications services regarding whom it has recognised compliance according to para 1, item 1;
2. the certificate for the electronic signature of the foreign provider of identification services for whom exists the responsibility according to para 1, item 2, the certificate for the electronic signature of the Bulgarian provider who has taken the responsibility, as well as the conditions under which the responsibility has been taken.

Chapter eight.
ADMINISTRATIVE PENAL PROVISIONS

Penalties
Art. 45. (1) Who violates or admits violation under art. 17, 18, art. 19, para 1, art. 21, para 1 and 3, art. 22, art. 24, para 1 and 2, art. 25, para 2, 3 and 5, art. 26, para 2, 3, 4, 5 and 6, art. 27, para 2, 3, art. 28, para 1, 2 and 3, art. 29, para 1, art. 30, para 1 shall be fined with 100 to 10 000 levs unless the act does not constitute a crime.

(2) In the cases under para 1 proprietary sanctions of 500 to 50 000 levs shall be imposed on the corporate body or sole entrepreneur.

Establishment of offences, issuance of acts and issuance of penalty decrees
Art. 46. (1) (Amend. SG 112/01) The acts for established offences shall be issued by persons authorised by the Chairman of the Commission for regulation of the communications and the penalty decrees shall be issued by him or by an official authorised by him.
(2) For established offences the issuers of acts can seize and hold the material evidence related to the establishment of the offences by the order of art. 41 of the Law for the administrative offences and penalties.
(3) The issuance of the acts, the issuance, appeal and fulfilment of the penalty decrees shall be carried out by the order of the Law for the administrative offences and penalties.

Additional provisions

§ 1. In the context of this law:
1. "Qualified written form" is a form of facts or proof of the statement whereas the law stipulates additional requirements for the written form, such as notary certification of the signature, a public notary act, manual writing of the statement, participation of witnesses or officials during the performance of the statement, etc.
2. "Asymmetric cryptographic system" is a system of cryptography of information allowing the creation and using of binary cryptographic key-words, including a private key-word and algorithmically connected public key-word with the following characteristics:
a) cryptography of one of the key can be made of the contents of a definite electronic statement and deciphering can be made by the other key-word;
b) it can be established, by using the public key-word, in an indisputable way, whether the transformation of the original electronic statement has been made by using the respective private key-word and whether the electronic statement has been changed after the transformation;
c) if one of the key-words is known it must be practically impossible to discover the other key-word.
3. "Cryptographic key-word" is a string of symbols used in an algorithm for transformation of information from comprehensible to coded type (cryptography) or vice versa - from coded to comprehensible type (decoding).
4. "Public key-word" is one of the couple of key-words used in asymmetric cryptographic system, which is accessible and can be used for verification of an electronic signature.
5. "Private key-word" is one of the couple of key-words used in asymmetric cryptographic system for creation of electronic signature.
6. "Mechanism of creating the signature" is a configured software or hardware used for introduction of data for creation of the signature.
7. "Data for creation of the signature" are a unique information, such as codes of cryptographic key-words used by the signing person for creation of electronic signature.

Concluding provisions

§ 2. Para 4 is created in art. 22 of the Law for the telecommunications (prom., SG 93/1998; amend. No 26/1999, No 10 and 64/2000):
"(4) (Amend. SG 112/01) The Commission for regulation of the communications shall register and control the activity regarding the providing of identification services by an order determined by a law."

§ 3. This law shall enter into force 6 months after its promulgation in the State Gazette.

§ 4. The Council of Ministers shall work out ordinances stipulated by this law within 5 months from its promulgation and shall adopt them within one month from the enactment of the law.

§ 5. (Amend. SG 112/01) The fulfilment of the law is assigned to the Council of Ministers and to the Commission for regulation of the communications.

The law was adopted by the 38th National Assembly on March 22, 2001 and was affixed with the official seal of the National Assembly.

Temporary and concluding provisions TO THE ADMINISTRATIVE PROCEDURE CODE

(PROM. – SG 30/06, IN FORCE FROM 12.07.2006)

§ 142. The code shall enter into force three months after its promulgation in State Gazette, with the exception of:

1. division three, § 2, item 1 and § 2, item 2 – with regards to the repeal of chapter third, section II "Appeal by court order", § 9, item 1 and 2, § 15 and § 44, item 1 and 2, § 51, item 1, § 53, item 1, § 61, item 1, § 66, item 3, § 76, items 1 – 3, § 78, § 79, § 83, item 1, § 84, item 1 and 2, § 89, items 1 - 4§ 101, item 1, § 102, item 1, § 107, § 117, items 1 and 2, § 125, § 128, items 1 and 2, § 132, item 2 and § 136, item 1, as well as § 34, § 35, item 2, § 43, item 2, § 62, item 1, § 66, items 2 and 4, § 97, item 2 and § 125, item 1 – with regard to the replacement of the word "the regional" with the "administrative" and the replacement of the word "the Sofia City Court" with "the Administrative court - Sofia", which shall enter into force from the 1st of May 2007;
2. paragraph 120, which shall enter into force from the 1st of January 2007;
3. paragraph 3, which shall enter into forcefrom the day of the promulgation of the code in State Gazette.

Concluding provisions TO THE LAW OF THE COMMERCIAL REGISTER

(PROM. – SG 34/06, IN FORCE FROM 01.10.2006)

§ 56. This law shall enter into force from the 1st of October, with the exception of § 2 and § 3, which shall enter into force from the day of the promulgation of the law in State Gazette.