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, ***amend. SG. 100/21 Dec 2010***

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) (supple. - SG 100/10, in force from 01.07.2011) Mediator of the electronic statement is a person who, by assignment of the titular, author or recipient, 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; amend. - SG 100/10, in force from 01.07.2011) to store the information under item 3 for a period of one year.
(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.

Confirmation of the receipt of the electronic statement (Title amend. - SG 100/10, in force from 01.07.2011)

Art. 8. (1) Confirmation of the receipt of the electronic statement shall not be required for deeming it received by the recipient, unless otherwise stipulated between the parties. Where the parties have stipulated that confirmation of the receipt is required and have not specified a time limit for that, the confirmation shall be made in a reasonable term.
(2) (revoked - SG 100/10, in force from 01.07.2011)
(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) (amend. - SG 100/10, in force from 01.07.2011) 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 specific information system the statement shall be considered received with its receipt in any 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.
(2) If confirmation has been stipulated, the electronic statement shall be received with the confirmation being sent by the recipient for its receipt.

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. (amend. - SG 100/10, in force from 01.07.2011) (1) Electronic signature shall be any information in electronic form, added to or logically related to the electronic statement, intended to establish its author.
(2) Improved electronic signature shall be an electronic signature, which:
1. makes possible the identification of the author;
2. is related in a unique way to the author;
3. is created by means which are under sole control of the author and
4. is related to the electronic statement in a way that makes it possible to establish any subsequent changes.
(3) Qualified electronic signature shall be an improved electronic signature meeting the requirements of Art. 16.
(4) The electronic signature under Para 3 shall be equal to a hand signature. The parties may stipulate to consider the value of the electronic signature under Para 1 and 2 equal to a hand signature in the relations between them.

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.
QUALIFIED ELECTRONIC SIGNATURE (TITLE AMEND. - SG 100/10, IN FORCE FROM 01.07.2011)

Section I.
General

Definition
Art. 16. (amend. - SG 100/10, in force from 01.07.2011) (1) Qualified electronic signature means an improved electronic signature which:
1. is accompanied by a certificate for qualified electronic signature issued by a certification service provider meeting the requirements of Art. 24 and certifying the link between the author and the public key for verification of the signature and
2. is created by a secure signature-creation device.
(2) The requirements to the algorithms for creation and verification of the qualified electronic signature shall be determined in an ordinance of the Council of Ministers.
(3) Qualified electronic signatures shall be:
1. the improved electronic signatures of the Commission for Regulation of the Communications for signing the acts pursuant to its duties under the law;
2. the improved electronic signatures of certification service providers.

Secure qualified electronic signature creation and verification device (Title amend. - SG 100/10, in force from 01.07.2011)
Art. 17. (amend. - SG 100/10, in force from 01.07.2011) (1) When creating a qualified electronic signature, the authors shall use a secure signature creation device, which shall guarantee that:
1. the data used for the creation of the electronic signature can be used only by its creation and their security is duly protected;
2. the data used for creation of the electronic signature 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 qualified electronic signature shall apply a mechanism guaranteeing that:
1. the data for verification of the electronic signature shall correspond to the data visualised before before the person carrying out the verification;
2. the signature shall be duly verified and the results from this verification have been visualised before the person carrying out the verification;
3. the contents of the signed statement can be duly established;
4. the authorship and validity of the electronic signature certificate have been duly verified at the moment of the check;
5. the results of the verification and the author's identity have been correctly reproduced;
6. the use of pseudonym has been clearly indicated;
7. all changes relate to security may be established.

Confidentiality of the private key-word
Art. 18. (revoked - SG 100/10, in force from 01.07.2011)

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. (supple. - SG 100/10, in force from 01.07.2011) issues certificates according to art. 24 and 40 and keep registers for them;
2. provides to every third person access to the published certificates.
(2) (amend. - SG 100/10, in force from 01.07.2011) The provider of identification services can provide services for creation of private and public key-word for qualified electronic signature.
(3) (new - SG 100/10, in force from 01.07.2011) The provider of identification services shall be a person carrying out public functions.

Organisations for voluntary accreditation

Art. 20. (revoked - SG 100/10, in force from 01.07.2011)

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. (amend. - SG 100/10, in force from 01.07.2011) maintaining available resources or have insurance which enable the fulfilment of the activities in compliance with the requirements of this law and cover non-fulfilment of their obligations under this law;
2. (revoked - SG 100/10, in force from 01.07.2011)
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. (amend. and supple. - SG 100/10, in force from 01.07.2011) 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 qualified electronic signatures, as well as good knowledge of the security procedures. The personnel shall exercise their duties in compliance with administration and management procedures established in accordance with generally accepted standards;
5. providing conditions for precise definition of the time of issuance, suspension, renewal and termination of the validity of the certificates;
6. (amend. - SG 100/10, in force from 01.07.2011) providing measures against forging the certificates, and where providing the creation of a private and public key service, they shall ensure the confidentiality of the process of creation of the data;
7. using reliable systems for storing and management of the certificates which ensure that:
a) (suppl. - SG 100/10, in force from 01.07.2011) only duly authorised employee have access for introduction of changes to the status of the certificates;
b) (amend. - SG 100/10, in force from 01.07.2011) establishment of the authenticity of the information;
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) (revoked - SG 100/10, in force from 01.07.2011)
8. (suppl. - SG 100/10, in force from 01.07.2011) providing the maintenance of a secure and reliable register and possibility of immediate stopping and termination of the validity of the certificates;
9. (Amend. SG 112/01; amend. - SG 100/10, in force from 01.07.2011) informing in advance the Commission for regulation of the communications about the starting of activity according to art. 19, Para 1;
10. (new - SG 100/10, in force from 01.07.2011) storing the entire information regarding the qualified signature certificates from the moment of receiving it for a term of 10 years.
(2) (amend. - SG 100/10, in force from 01.07.2011) The Council of Ministers shall adopt ordinance under para 1, item 1 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. (amend. - SG 100/10, in force from 01.07.2011) to issue certificate upon request of every person informing him in advance whether he is accredited;
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. (amend. - SG 100/10, in force from 01.07.2011) when issuing certificates to verify through the admissible means the personality, respectively the identity, of the author and of the titular of the qualified electronic signature and, where necessary - other data regarding these persons, included in the certificate;
4. (suppl. - SG 100/10, in force from 01.07.2011) to publish the issued certificate so that third persons can have access to it according to the instructions of the author, respectively 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. (revoked - SG 100/10, in force from 01.07.2011)

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 qualified electronic signature (Title amend. - SG 100/10, in force from 01.07.2011)

Certificate

Art. 24. (1) (amend. - SG 100/10, in force from 01.07.2011) The certificate is an electronic document, issued and signed by the provider of identification services containing:
1. indication that the certificate has been issued for a qualified electronic signature;
2. the name and the address of the identification service provider and indication of the country of his business establishment;
3. the name or pseudonym of the author of the electronic signature;
4. special indications related to the author if the certificate is issued for a certain purpose and also when the provider has a policy for issuing certificates with such indications;
5. the public key corresponding to the private key held by the author for creation of a qualified electronic signature
6. the transformed electronic signature of the identification service provider;
7. the term of validity of the certificate;
8. the limitations of the effect of the signature in terms of the objectives and/or value of the transactions, where the issued certificate has limited identification effect;
9. the unique identification code of the certificate;
10. mention of the accreditation the provider, if accredited.
(2) (revoked - SG 100/10, in force from 01.07.2011)
(3) (revoked - SG 100/10, in force from 01.07.2011)
(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. (amend. - SG 100/10, in force from 01.07.2011) it originates from the author or from a person duly authorised by him;
2. (amend. - SG 100/10, in force from 01.07.2011) the information regarding the author, presented for inclusion in the certificate, is correct and full, and
3. the private key-word:
a) (amend. - SG 100/10, in force from 01.07.2011) is held by the author;
b) (amend. - SG 100/10, in force from 01.07.2011) is technically fit to be used for creation of a qualified electronic signature, and
c) (amend. - SG 100/10, in force from 01.07.2011) corresponds to the public key-word, so that it can be certified through the public key-word that a definite qualified electronic signature is created by the private key-word.
(3) (amend. - SG 100/10, in force from 01.07.2011) Where the request is for entry into the certificate of a holder on behalf of whom will be made the statements, the application shall be upheld, if the requirements of Para 2,

Items 2 and 3 have been met, and:
1. the application originates from the holder of a person duly authorised by him, and
2. the information about the holder, presented for inclusion in the certificate, is correct and complete.
(4) (revoked - SG 100/10, in force from 01.07.2011)
(5) (amend. - SG 100/10, in force from 01.07.2011) The provider of identification services shall issue immediately the certificate by publishing it in the register of certificates.
(6) (new - SG 100/10, in force from 01.07.2011) The author, respectively the holder, may contest within three days from the publication in the register, if the issued certificate contains errors or omissions. They shall be immediately rectified by the provider by issuing a new certificate without payment, unless they have been caused by provision of incorrect information. The lack of contest shall be deemed to consider the contents of the certificate approved.

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. (amend. and suppl. – SG 100/10, in force from 01.07.2011) upon request of the author or titular, respectively the author, without being obliged to establish the identity or the power of representation of the author;
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) (amend. – SG 100/10, in force from 01.07.2011) The provider of identification services shall immediately inform the author and the titular about the suspension of the validity of the certificate.
(5) (amend. – SG 100/10, in force from 01.07.2011) The suspension of the validity of the certificate shall be carried out by its temporary entry into the list of the terminated certificates.
(6) The validity of the certificate shall be renewed by:
1. the expiration of the term of suspension;
2. (Amend. SG 112/01; suppl. – SG 100/10, in force from 01.07.2011) by the provider of identification services - upon dropping the grounds for suspension or upon request of the author or 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.
(7) (new – SG 100/10, in force from 01.07.2011) The renewal of the certificate's validity shall annul the consequences of the suspension.

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) (amend. – SG 100/10, in force from 01.07.2011) 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 their identity and the representative authority of the author.
(3) The supplier of identification services shall terminate the validity of he certificate upon:
1. (amend. – SG 100/10, in force from 01.07.2011) death or placing under judicial disability of the author or the titular;
2. (suppl. – SG 100/10, in force from 01.07.2011) termination of the corporate body of the titular, if a titular has been entered upon the issuance of the certificate;
3. (suppl. – SG 100/10, in force from 01.07.2011) termination of the representative authority of the author regarding the titular if a titular has been entered upon the issuance of the certificate;
4. establishing that the certificate has been issued on the grounds of false data.
(4) (new – SG 100/10, in force from 01.07.2011) The terminated certificates pursuant to Para 3 shall be entered in

the list of terminated certificates kept buy the identification service provider. The provider shall enter the certificates with terminated validity into the list immediately after being notified of the relevant circumstances.

Register of the certificates

Art. 28. (1) (amend. – SG 100/10, in force from 01.07.2011) The provider of identification services shall keep an electronic register where he shall publish the electronic signature certificates issued by him as a provider, the issued certificates and the list of the terminated certificates.
(2) (amend. – SG 100/10, in force from 01.07.2011) The provider of identification services cannot restrict the access to the register except upon request by the author in respect of his signature certificate.
(3) The provider of identification services shall publish in the register under para 1 information for:
1. (amend. – SG 100/10, in force from 01.07.2011) the conditions and the order of issuing certificate, including for the rules of establishing the identity of the titular of the qualified electronic signature;
2. the security procedures of the provider of identification services;
3. (amend. – SG 100/10, in force from 01.07.2011) the way of using the qualified electronic signature;
4. (amend. – SG 100/10, in force from 01.07.2011) the conditions and the order of using the qualified electronic signature, including the requirements for storing the private key-word;
5. (amend. – SG 100/10, in force from 01.07.2011) the conditions of access to the certificate and the way of verification of the qualified 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. (amend. – SG 100/10, in force from 01.07.2011) the responsibility of the provider of identification services and of the titular of the qualified electronic signature;
8. (amend. and suppl. – SG 100/10, in force from 01.07.2011) the conditions and the order by which the author, respectively the titular, extends request for termination of the validity of the qualified 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) (amend. and suppl. – SG 100/10, in force from 01.07.2011) The provider of identification services shall be responsible before the author, respectively before the titular of the qualified 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. (amend. – SG 100/10, in force from 01.07.2011) from the algorithmic non-compliance between the private key and the public key entered into the certificate.
(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 author and of the holder to third persons (Title amend. – SG 100/10, in force from 01.07.2011)

Art. 30. (1) (amend. – SG 100/10, in force from 01.07.2011) The author 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 2.
(2) (amend. – SG 100/10, in force from 01.07.2011) The author shall be responsible to the third conscientious persons if:
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) (amend. – SG 100/10, in force from 01.07.2011) The author shall be responsible to the third conscientious persons for false statements made before the provider of identification services and related to the contents or the issuance of the certificate.

(4) (amend. – SG 100/10, in force from 01.07.2011) Where a titular has been entered upon the issuance of the certificate, he shall be liable for any default by the author related to his duties under Para 1 – 3.

Responsibility of the titular and of the author to the provider of identification services

Art. 31. (amend. – SG 100/10, in force from 01.07.2011) The author, respectively the titular, shall be responsible before the provider of identification services if the author has provided false data or has failed to reveal data related to the contents or to the issuance of the certificate, and where he has not held the private key corresponding to the public key indicated in the certificate.

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. (revoked – SG 100/10, in force from 01.07.2011)
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.

Suspension of the activity of issuance of qualified electronic signature certificates

Art. 32a. (new – SG 100/10, in force from 01.07.2011) (1) The Commission for Regulation of the Communications may suspend in a decision the activity of any identification service provider related to the issuance of qualified electronic signature certificates in breach of the law and the subordinate normative acts until discontinuance of the breach.
(2) The appeal of the decision referred to in Para 1 shall not suspend its execution.

Chapter four.
ACCREDITATION AND CONTROL (TITLE AMEND. – SG 100/10, IN FORCE FROM 01.07.2011)

Definition

Art. 33. (revoked – SG 100/10, in force from 01.07.2011)

Accredited institution (Title amend. – SG 100/10, in force from 01.07.2011)

Art. 34. (Amend. SG 112/01; amend. – SG 100/10, in force from 01.07.2011) (1) The Executive Agency "Bulgarian Service for Accreditation" shall accredit the identification service provider.

Powers of the Executive Agency "Bulgarian Service for Accreditation" in Respect of the Providers (Title amend. SG 112/01; amend. – SG 100/10, in force from 01.07.2011)

Art. 35. (Amend. SG 112/01; amend. – SG 100/10, in force from 01.07.2011) (1) The Executive Agency "Bulgarian Service for Accreditation" shall:

1. accredit the providers of identification services;
2. refuse accreditation of providers of identification services when they do not meet the necessary requirements;
3. withdraw the accreditation of the providers of identification services.
(2) The Executive Agency “Bulgarian Service for Accreditation” shall issue certificates of the accredited identification service providers.

Accreditation of the providers of identification services (Title amend. – SG 100/10, in force from 01.07.2011)

Art. 36. (amend. – SG 100/10, in force from 01.07.2011) The sector scheme for voluntary accreditation of the certification service providers, the conditions and order for accreditation, the surrender of accreditation and the withdrawal of accreditation shall be set out in an ordinance of the executive director of the Executive Agency “Bulgarian Service for Accreditation”.

Deletion of the registration

Art. 37. (revoked – SG 100/10, in force from 01.07.2011)

Termination of the activity of an identification service provider

Art. 37a. (new – SG 100/10, in force from 01.07.2011) The termination of the activity of an identification service provider shall be regulated in the ordinance referred to in Art. 32, Para 4.

Register of the providers of identification services

Art. 38. (amend. - SG 100/10, in force from 01.07.2011) (1) The Commission for Regulation of the Communications shall maintain a register of all providers located on the territory of the Republic of Bulgaria that have notified it of the commencement of their activity under Art. 19, Para 1 and of the accredited providers.
(2) The Register of the providers of identification services shall be public.
(3) The Commission for Regulation of the Communications shall publish in the register the basic and operational electronic signature certificates of providers of identification services and its basic and operational certificates under Art. 16, Para 3, Item 1.
(4) (In force from 21.12.2010) The maintenance, storage and access to the register shall be regulated in an ordinance of the Commission for Regulation of the Communications, which shall be promulgated in the State Gazette.

State fees

Art. 39. (1) (amend. - SG 100/10, in force from 01.07.2011) For accreditation of the providers of identification services and for the issuance of certificates 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.

Time certificates (Title amend. - SG 100/10, in force from 01.07.2011)

Art. 40. (amend. - SG 100/10, in force from 01.07.2011) (1) The identification service provider may issue a certificate about the time of provision of an electronic signature created for a certain electronic document.
(2) The time certificate shall be a electronic document signed by the identification service provider containing at least:
1. the identifier of the policy for issuing time certificates which is part of the user handbook of the identification service provider that has issued the time certificate;
2. the electronic signature of the signed electronic document submitted to the provider;
3. the identifiers of the algorithms used for the creation of the electronic signature;
4. the time of provision of the electronic signature;
5. the unique identification number of the time certificate;
6. the qualified electronic signature certificate of the identification service provider that has issued the time certificate, or the corresponding reference thereto.
(3) The time certificate shall have the effect of official identification after its entry into a register of the issued time certificates maintained by the provider. The requirements to the maintenance and storage of the register shall be determined in the ordinance under Art. 28, Para 4.
(4) The identification service provider shall publish into the register under Para 3 also the information applicable to the certificates about the circumstances referred to in Art. 28, Para 3.
(5) The requirements to the time certificates, the form and the rules for their issue shall be determined in the ordinance under Art. 32, Para 4.
(6) The provider shall publish in the register under Art. 28 the electronic signature certificates issued in the course of his activity for issue of time certificates.

Chapter five.
APPLICATION OF THE ELECTRONIC DOCUMENT AND OF THE QUALIFIED ELECTRONIC SIGNATURE BY THE STATE AND THE MUNICIPALITIES (TITLE AMEND. - SG 100/10, IN FORCE FROM 01.07.2011)

Obligation for acceptance and issuance of electronic documents

Art. 41. (revoked - SG 100/10, in force from 01.07.2011)

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) (amend. - SG 100/10, in force from 01.07.2011) 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 maintenance of electronic signature certificates.
(4) (amend. - SG 100/10, in force from 01.07.2011) Personal data may be gathered only personally from the person they concern or by his explicit consent.
(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. (amend. - SG 100/10, in force from 01.07.2011) (1) Qualified electronic signature certificates issued by providers of identification services established in other Member States of the European Union or in a contracting party to the Agreement on the European Economic Area shall be recognised as equal to certificates issued by a Bulgarian provider of certification services.
(2) Qualified electronic signature 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 accredited in a Member State of the European Union or in a contracting party to the Agreement on the European Economic Area;
2. a provider of identification services established in a Member State of the European Union or in a contracting party to the Agreement on the European Economic Area 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 between the European Union and third countries or international organisations or by an international agreement between the Republic of Bulgaria and a third country.
(3) The conditions under para 2, items 1 and 2 shall be specified by the Commission for regulation of the communications by the publishing in separate lists in the register under Art. 38 maintained by it of:
1. the foreign providers of identifications services which certificates are recognised under the conditions of Para 2;
2. the name of the provider that has undertaken the responsibility under the conditions of Para 2, Item 2, as well as the conditions for undertaking the responsibility.

Chapter eight.
ADMINISTRATIVE PENAL PROVISIONS

Penalties

Art. 45. (1) (amend. - SG 100/10, in force from 01.07.2011) Who violates or admits violation under 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 1000 to 50 000 levs unless the act does not constitute a crime.
(2) (amend. - SG 100/10, in force from 01.07.2011) In the cases under para 1 proprietary sanctions of 5000 to 100 000 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. (amend. - SG 100/10, in force from 01.07.2011) "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. (amend. - SG 100/10, in force from 01.07.2011) "Device for safe creation of 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;
8. (new - SG 100/10, in force from 01.07.2011) "Signature-verifiation data" means unique data, such as codes or private cryptographic keys, which are used by the verifying person to verify an electronic signature.
9. (new - SG 100/10, in force from 01.07.2011) "Signature-secure-verification device" means configured software or hardware used to implement the signature-verification-data;
10. (new - SG 100/10, in force from 01.07.2011) "Basic electronic signature certificate" means an electronic signature certificate issued by an identification service provider to himself that certified the public key used for verification of the operational electronic signature certificates signed by the identification serve provider.
11. (new - SG 100/10, in force from 01.07.2011) "Operational electronic signature certificate" means an electronic signature certificate issued by an identification service provider to himself and signed by an electronic signature accompanied by a basic electronic signature certificate. The operation certificate shall identify the public key used for verification of the electronic signature certificates and time certificates issued to consumers and signed by the identification service provider.

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.

Transitional 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.

Additional provisions
S TO THE LAW ON AMENDMENT AND SUPPLEMENTATION OF THE LAW ON THE ELECTRONIC DOCUMENT AND THE ELECTRONIC SIGNATURE
(PROM. - SG 100/10, IN FORCE FROM 21.12.2010)

§ 40. This Law shall implement the requirements of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, amended by Regulation (EC) 1137/2008.

Transitional and concluding provisions
TO THE LAW ON AMENDMENT AND SUPPLEMENTATION OF THE LAW ON THE ELECTRONIC DOCUMENT AND THE ELECTRONIC SIGNATURE
(PROM. - SG 100/10, IN FORCE FROM 21.12.2010)

§ 41. (1) The identification service providers registered by the Commission for Regulation of the Communications shall be deemed accredited in the sense of this Law.
(2) The Commission for Regulation of the Communications shall enter ex officio into the register under Art. 38, Para 1 the circumstances related to the accreditation of the identification service providers registered before entry

into force of this Law.

§ 42. All certificates for enhanced and universal electronic signature issued before entry into force of this Law shall be deemed equal to qualified electronic signature certificates.
……..

§ 52. The Commission for Regulation of the Communications shall adopt the ordinance under Art. 38, Para 4 by 1 March 2011.

§ 53. The subordinate normative acts on the implementation of this Law shall be made compliant with the requirements of this Law by 1 July 2011.

§ 54. This Law shall enter into force from 1 July 2011 except for the provision of § 31 regarding Art. 38, Para 4, which shall enter into force from the day of its promulgation in the State Gazette.

Relevant acts of the European Legislation

Directive 2003/58/EC of the European Parliament and of the Council of 15 July 2003 amending Council Directive 68/151/EEC, as regards disclosure requirements in respect of certain types of companies
Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
Regulation (EEC) No 2380/74 of the Council of 17 September 1974 adopting provisions for the dissemination of information relating to research programmes for the European Economic Community