

LAW ON ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE
(Promulgated, SG 34/2001)

Chapter one
GENERAL PROVISIONS

Scope of Applicability

Article 1

(1) This Act shall regulate electronic document, electronic signature and terms and procedure for providing certification services.

(2) This Act shall not apply:

1. for transactions, for which the law requires a qualified written form;
2. when the act of holding of a document or a copy of it has any legal significance (securities, bills of lading, other).

Chapter two
ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE

Electronic Statement

Article 2

(1) Electronic statement shall be a verbal statement, represented in a digital form through a common standard for transformation, reading and visual representation of information.

(2) The electronic statement may contain as well nonverbal information.

Electronic Document

Article 3

(1) Electronic document shall be an electronic statement, recorded on magnetic, optical or other carrier that allows it to be reproduced.

(2) The written form shall be considered observed if an electronic document has been composed.

Signatory and Owner of an Electronic Statement

Article 4

Signatory of an electronic statement shall be the natural person that is named in the statement as its performer. Owner of an electronic statement shall be the person on behalf of whom the electronic statement has been performed.

Addressee of an Electronic Statement

Article 5

Addressee of an electronic statement may be a person that by virtue of a Law is obliged to receive electronic statements or that according to unambiguous circumstances may be considered to have agreed to receive the statement in an electronic form.

Intermediary of an Electronic Statement

Article 6

(1) Intermediary of an electronic statement shall be a person that upon assignment by the owner sends, receives, records, or stores an electronic statement or performs other services, related to it.

- (2)** The intermediary of an electronic statement shall be obliged:
1. to have technical and technological equipment that is to ensure the trustworthiness of the used systems;
 2. to maintain staff that has the necessary expert knowledge, experience and qualification;
 3. to ensure conditions for exact determination of the time and source of the transferred electronic statements;
 4. to use trustworthy systems for the storage of the information under Point 3;
 5. to store the information under Point 3 for a term of six months.
- (3)** The intermediary of an electronic statement shall be liable for damages caused by non-performance of his or her obligations under Paragraph 2.

Mistake in Transferring an Electronic Statement

Article 7

The owner shall take the risk of mistakes in transferring the electronic statement, unless the addressee has not exercised reasonable care.

Receipt of an Electronic Statement

Article 8

- (1)** The electronic statement shall be considered received if the addressee confirms the receipt.
- (2)** If no time for confirmation of receipt has been specified the confirmation should be made in a reasonable time.
- (3)** The confirmation of receipt shall not certify the content of the electronic statement.

Time of Sending an Electronic Statement

Article 9

The electronic statement shall be sent with its entering into an information system that is not under the control of the signatory.

Time of Receiving an Electronic Statement

Article 10

- (1)** The electronic statement shall be received with the sending of a confirmation for its receipt by the addressee.
- (2)** If a confirmation is not required, the electronic statement shall be received with its entering into the information system, specified by the addressee. If the addressee has not specified an information system, the statement shall be received with its entering into an information system of the addressee, and if the addressee does not have an information system - with its retrieving by the addressee from the information system it has entered into.

Time of Electronic Statement Acquiring

Article 11

The addressee of the electronic statement shall be considered to have acquired the content of the statement in a reasonable time since its receipt.

Place of Sending and Receiving an Electronic Statement

Article 12

- (1)** The electronic statement shall be considered sent from the place of

business of its owner.

(2) The electronic statement shall be considered received in the place of business of its addressee.

(3) If the owner or the addressee of the statement has more than one place of business, the place of business shall be considered to be the one that is most closely related to the statement and its performance, with taking into account the circumstances, which the owner and the addressee have known or have taken into consideration at any time before or during the performance of the statement.

(4) If the owner or the addressee does not have a place of business, their permanent residence shall be taken into consideration.

Electronic Signature

Article 13

(1) Electronic signature shall be:

1. any information, related to the electronic statement in a way, concerted between the signatory and the addressee, secure enough in view of the turnover needs, that:

- a) reveals the identity of the signatory;
 - b) reveals the consent of the signatory with the electronic statement; and
 - c) protects the content of the electronic statement from subsequent changes.
2. an advanced electronic signature;
3. an universal electronic signature.

(2) An electronic signature under Points 1 and 2 shall have an effect of a handwritten signature, unless the owner or the addressee of an electronic statement is a state authority or a local self-government authority.

(3) An universal electronic signature shall have an effect of a handwritten signature towards everyone. The Council of Ministers shall specify the state authorities that may use another type of electronic signature in their relations.

Secrecy of a Signature-Creation Data

Article 14

No one except for the signatory shall have the right of access to the signature-creation data.

Contesting an Electronic Signature

Article 15

(1) The person, indicated as an owner or a signatory of the electronic statement, may not contest the authorship in relation to the addressee, if the statement has been signed with an electronic signature, and:

1. the statement has been sent through an information system, designed to work in an automatic regime; or
2. the statement has been performed by a person, to whom an access to the method of identification has been given.

(2) Paragraph 1, Point 2 shall not apply from the moment the addressee receives a notification that the electronic statement does not come from the signatory and the addressee has enough time to adapt his or her behavior to the notification.

(3) Paragraph 1 shall not apply when the addressee of the statement has not exercised reasonable care.

Chapter three
ADVANCED ELECTRONIC SIGNATURE

Part I
General Provisions

Definition

Article 16

(1) Advanced electronic signature shall be a transformed electronic statement, included, added or logically related to the same electronic statement before its transformation.

(2) The transformation under Paragraph 1 is done through algorithms, including the use of the private key of an asymmetric cryptosystem.

(3) The requirements to the algorithms shall be defined in a Regulation of the Council of Ministers.

Mechanism for Creation and Verification of an Advanced Electronic Signature

Article 17

(1) Persons, creating an advanced electronic signature should apply a mechanism guaranteeing, that:

1. the signature-creation data can occur only during the electronic signature creation and the secrecy of the data is reasonably assured;
2. the signature-creation data is not accessible, cannot be derived and the signature is protected against forgery;
3. the signature-creation data can be protected by the signatory against the use of others;
4. the content of the statement is made available to the signatory and remains unaltered until the creation of the electronic signature.

(2) Persons, verifying an advanced electronic signature should apply a mechanism guaranteeing, that:

1. the data ascertaining the use of the private key corresponds to the data, given to the person, using the public key;
2. the use of the private key has been reliably verified and the results of that verification have been given to the person that had used the public key.

Secrecy of the Private Key

Article 18

No one except for the signatory shall have the right of access to the private key.

Part II
Certification-Service-Providers

Activities of the Certification-Service-Providers

Article 19

(1) Certification-service-provider shall be a person, that:

1. issues certificates under Article 24 and keeps their registry;
2. provides a third person with access to the certificates that have been published.

(2) The certification-service-provider may offer services on the creation of the advanced electronic signature private and public key.

Organizations for Voluntary Accreditation

Article 20

(1) Certification-service-providers may set up organizations for voluntary accreditation aiming to achieve higher level in the certification services they offer.

(2) The organizations for voluntary accreditation assist the acknowledgement of the legal effect of certificates, issued by the Bulgarian service-providers abroad, and also certificates issued by the foreign service-providers in Bulgaria.

(3) Conditions for participation in the organizations for voluntary accreditation should be widely accessible and should create equality among all certification-service-providers.

Requirements towards Activities of the Certification-Service-Providers

Article 21

(1) Certification-service-providers perform their activities, while:

1. maintaining available resources that are to ensure performance of their activities in accordance with the requirements of this Law;
2. insuring themselves for the time of their activities against the damages caused by non-performance of their obligations under this Law;
3. having technical equipment and technology, that is to ensure the trustworthiness of the used systems and technical and cryptographic security of the processes they perform;
4. keeping staff that has the necessary expert knowledge, experience and qualification for the performance of activities, especially in the area of advanced electronic signatures technology, and also good level of understanding of the security procedures;
5. ensuring conditions for exact determination of the time of issuance, suspension, renewal, and revocation of the effect of the certificates;
6. ensuring measures against the forgery of certificates and for the confidentiality of the data they have access to in the process of signature creation;
7. using trustworthy systems for storage and administration of certificates, that are to ensure:
 - a) that only duly authorized employees have access to make changes;
 - b) that the authenticity and validity of the certificates can be ascertained;
 - c) possibility for a limited access to the published certificates;
 - d) any appearance of technical problems in relation to security to be made known immediately to the staff;
 - e) possibility for the private key confirmation to be canceled with the expiration of the term of the certificate.
8. ensuring possibility for immediate suspension and revocation of the effect of the certificates.
9. immediately informing the State Telecommunications Commission on the beginning of activities under Article 19.

(2) The Council of Ministers shall adopt Regulation under Points 1, 2 and 3 of Paragraph 1.

(3) The certification-service-provider may not use the information it stores for purposes, different from the ones, relating to its activities. It may give to third parties only the information, included in the certificates.

Obligations of the Certification-Service-Provider

Article 22

The certification-service-provider shall be obliged:

1. to issue a certificate upon request by any person, while prior to that the certification-service-provider has to inform that person if it has been registered under the procedure of Chapter Four and whether it is participating in the organizations for voluntary accreditation;
2. to inform persons, willing to have a certificate issued, on the terms for issuance and use of the certificate, including the restrictions of its effect, as well as on the procedures for complaints submission and disputes resolution;
3. when issuing certificates, to examine by admissible means, the identity of the signatory and the owner of the advanced electronic signature and, if necessary, any other data about these persons, included in the certificate;
4. to publish the certificate that has been issued, so as third parties to have access to it according to the instructions of the owner;
5. not to store or copy data used for the creation of private keys;
6. to undertake immediate actions in relation to the suspension, renewal, and revocation of the effect of the certificate, when finding the relative grounds for it;
7. immediately to inform the owner and the signatory on circumstances relating to the validity or trustworthiness of the issued certificate;
8. to possess an advanced electronic signature, that is to be used only in relation to its activities as a certification-service-provider.

Relations with the Owner

Article 23

The relations between the certification-service-provider and the owner shall be regulated by a written contract.

Part III

Advanced Electronic Signature Certificates

Certificate

Article 24

(1) Certificate shall be an electronic document, issued and signed by a certification-service-provider that includes:

1. the name, address, personal identification number (PIN) or BULSTAT of the certification-service-provider, as well as an indication of its nationality;
2. the name or the trade name, address and court registration data of the owner of the advanced electronic signature;
3. the grounds for authorization, the name and address of the natural person (signatory) that is authorized to make electronic statements on behalf of the owner of the advanced electronic signature;
4. the public key that corresponds to the private key of the owner of the advanced electronic signature;
5. the identifications of algorithms with the help of which the public keys of the

- owner of the advanced electronic signature and of the certification-service-provider are used;
6. the date and the hour of issuance, suspension, renewal, and revocation of the effect;
 7. the term of validity;
 8. the restrictions of the effect of the signature;
 9. the unique identification code of the certificate;
 10. the liability and guarantees of the certification-service-provider;
 11. reference to the advanced electronic signature certificate under Article 22, Point 8 of the certification-service-provider and to its registration at the State Telecommunications Commission.
- (2)** When the authorization of the signatory comes from other authorized persons the certificate should include the data under Point 2 of Paragraph 1 for these persons.
- (3)** Unless something else has been agreed the certificate shall have effect for a period of three years.
- (4)** The owner and the signatory are obliged to inform immediately the certification-service-provider for any changes in the circumstances, indicated at the certificate.
- (5)** Changes in the circumstances, indicated in the certificate, cannot be opposed to third conscientious parties.

Issuance of a Certificate

Article 25

- (1)** The certification-service-provider shall issue a certificate upon a written request from the owner.
- (2)** The request under Paragraph 1 shall be satisfied, if:
1. it comes from the owner or a person, duly authorized by him or her;
 2. the information concerning the owner, presented to be included in the certificate is veracious and complete; and
 3. the private key:
 - a) is held by the owner;
 - b) is technically usable for the creation of an advanced electronic signature; and
 - c) corresponds to the public key, so that through the public key it can be certified that certain advanced electronic signature has been created using the private key.
- (3)** If the requested certificate concerns an advanced electronic signature of a signatory, different from the owner, the request shall be satisfied, if the requirements under Paragraph 2 have been observed, and:
1. the information presented to be included in the certificate concerning the signatory is also veracious and complete; and
 2. the signatory holds the private key.
- (4)** With the fulfillment of the request the certification-service-provider shall demand from the owner, respectively from the signatory, to accept the content of the requested certificate. It shall change the content of the certificate, if the owner, respectively the signatory, points out inexactness or incompleteness.
- (5)** The certification-service-provider shall immediately issue the certificate, the content of which has been accepted under the procedure of Paragraph 4 through its publication in the registry of certificates.

Suspension and Renewal of the Effect of the Certificate

Article 26

(1) Unless something else has been agreed, the certification-service-provider shall have the right to suspend the effect of a certificate, it has issued, for a term needed under the circumstances, but for no more than 48 hours, if there exists a well-founded doubt that the effect of the certificate has to be revoked.

(2) Unless something else has been agreed, the certification-service-provider shall be obliged to suspend the effect of a certificate, issued by it, for a term needed under the circumstances, but for no more than 48 hours:

1. upon a request from the owner, respectively from the signatory, without having an obligation to convince itself in his or her identity or representative authority;
2. upon a request from a person, for whom it is obvious under the circumstances that he or she may know as an agent, partner, employee, member of the family, etc., about infringements of the security of the private key;
3. upon a request from the State Telecommunications Commission.

(3) In case of a present danger for the interests of third parties or in case of existence of enough data about the violation of the law, the Chair of the State Telecommunications Commission may oblige the certification-service-provider to suspend the effect of the certificate for a term needed under the circumstances, but for no more than 48 hours.

(4) The certification-service-provider shall immediately notify the owner and the signatory about the suspension of the effect of the certificate.

(5) The suspension of the effect of the certificate shall be made through making the access to it impossible.

(6) The effect of the certificate shall be renewed:

1. with the expiration of the term of suspension;
2. by the certification-service-provider in case of dropping out of the ground for suspension or upon a request from the owner after the certification-service-provider, respectively the State Telecommunications Commission, have convinced themselves that he or she has learned of the cause for suspension as well as that the request for renewal has been made in consequence of learning.

Revocation of the Effect of the Certificate

Article 27

(1) The effect of the certificate shall be revoked:

1. with the expiration of the term;
2. with the death or placing under legal incapacity of the natural person - certification-service-provider;
3. with the dissolution of the legal person of the certification-service-provider without transferring its activities to another certification-service-provider.

(2) The certification-service-provider shall be obliged to revoke the effect of the certificate upon a request from the owner or the signatory after it has convinced itself in the identity and representative authority of the owner, respectively the signatory.

(3) The certification-service-provider shall revoke the effect of the certificate in case of:

1. death or placing under legal incapacity of the owner or the signatory;
2. dissolution of the legal person of the owner;
3. revocation of the representative authority of the signatory towards the owner;
4. ascertaining that the certificate has been issued on the basis of false data.

Registry of Certificates

Article 28

(1) The certification-service-provider shall maintain an electronic registry in which it publishes its own electronic signature certificate under Point 8 of Article 22, and the other issued certificates.

(2) The certification-service-provider cannot limit the access to the registry. Only the signatory can limit the access to his/her signature certificate.

(3) The certification-service-provider shall also publish in the registry under Paragraph 1 information about:

1. the terms and procedure for issuance of a certificate, including the rules for ascertaining the identity of the owner of an advanced electronic signature;
2. the security procedures of the certification-service-provider;
3. the way of using the advanced electronic signature;
4. the terms and procedure for using the advanced electronic signature, including the requirements for storing the private key;
5. the conditions for access to the certificate and the ways of checking the advanced electronic signature;
6. the price for receiving and using a certificate, as well as the prices of the other services, provided by the certification-service-provider;
7. the liability of the certification-service-provider and the owner of an advanced electronic signature;
8. the terms and procedure under which the owner makes a request for revocation of the effect of an advanced electronic signature.

(4) The method for maintaining the registry under Paragraph 1 shall be regulated with a Regulation of the Council of Ministers.

Part IV Liability

Liability of the Certification-Service-Provider

Article 29

(1) The certification-service-provider shall be liable before the owner of the advanced electronic signature and all third parties for the damages caused:

1. by non-performance of the requirements under Article 21 and of the obligations under Article 22 and 25;
2. from false or missing data in the certificate at the moment of its issuance;
3. to them in case that during the issuance of the certificate the person, pointed as a signatory, has not disposed of the private key, corresponding to the public key;
4. by non-correspondence of the data for the use of the private key and the data disposed to the person using the public key.

(2) The agreements by which the certification-service-provider's liability for negligence is excluded or limited shall be invalid.

(3) The certification-service-provider shall not be liable for damages, caused

by the use of the certificate beyond the limits of restrictions of its effect, listed in it.

Liability of the Owner and the Signatory towards Third Parties

Article 30

(1) The owner shall be liable towards conscientious third parties, when during the creation of the key pair (public and private key) an algorithm not corresponding to the requirements of the Regulation under Article 16, Paragraph 3 has been used.

(2) The owner shall be liable towards conscientious third parties, if the signatory:

1. does not perform exactly the security requirements, specified by the certification-service-provider;
2. does not request from the certification-service-provider revocation of the certificate, when he has learned that the private key has been used illegally or a danger of its illegal use exists.

(3) The owner, who has accepted the certificate with its issuance, shall be liable towards conscientious third parties:

1. if the signatory is not authorized to hold the private key corresponding to the public key pointed in the certificate;
2. for false statements made before the certification-service-provider that are related to the content of the certificate.

(4) The signatory, who has accepted the certificate with its issuance, shall be liable towards conscientious third parties, if he has not been authorized to request the issuance of the certificate.

Liability of the Owner and the Signatory towards the Certification-Service-Provider

Article 31

The owner, respectively the signatory, shall be liable towards the certification-service-provider, if he or she has accepted the certificate, issued by the certification-service-provider on the basis of false data, presented by him or her, respectively on the basis of data concealed by him or her.

Part V Regulation and Control

Powers of the State Telecommunications Commission

Article 32

(1) The State Telecommunications Commission shall have the following powers:

1. to exercise control over the certification-service-providers concerning the trustworthiness and security of the certification services;
2. to approve the manuals for the consumers and the prescribed security procedures;
3. to work out, co-ordinate and propose to the Council of Ministers for adoption draft Regulations under this Law and also concerning:
 - a) The regulation of the activities of the registered certification-service-providers and the procedure for termination of their activities;
 - b) The requirements concerning the format of certificates issued by the

certification-service-providers;

c) The requirements for the storage of information on the services provided by the certification-service-providers;

d) The requirements for the content, form and sources in relation to the information disclosed by the certification-service-providers;

(2) In the performance of its functions the State Telecommunications Commission shall have the right:

1. of free access to the objects liable to control;

2. to examine the documents proving the qualification of the staff of the certification-service-providers;

3. to request information and documents related to the exercise of control;

4. to determine persons that would control the fulfillment of the requirements of Article 17 and Article 21, Paragraph 1 by the certification-service-providers.

(3) The State Telecommunications Commission shall maintain and publish the list of persons under Paragraph 2, Point 4.

(4) The activities of the certification-service-providers and the procedure for termination of their activities, the requirements concerning the format of certificates issued by the certification-service providers, the requirements for the storage of information on the services provided by the certification-service-providers, the requirements for the content, form and sources in relation to the information disclosed by the certification-service-providers, the requirements towards persons under Paragraph 2, Point 4 as well as procedure and conditions for their inclusion in the list under Paragraph 3 shall be defined in a Regulation of the Council of Ministers.

Chapter four UNIVERSAL ELECTRONIC SIGNATURE

Definition

Article 33

(1) Universal electronic signature shall be an advanced electronic signature, the certificate for which is issued by the certification-service-provider, registered under Article 34.

(2) Universal electronic signature shall be also:

1. the electronic signature of the State Telecommunications Commission, with which it signs acts, issued on the basis of its powers, determined by the law.

2. electronic signatures under Point 8 of Article 22 of the registered certification-service-providers.

Registry Institution

Article 34

(1) The State Telecommunications Commission registers the certification-service-providers and keeps the registry of their advanced electronic signature certificates under Article 22, Point 8.

(2) The State Telecommunications Commission publishes at the registry under Paragraph 1 its own advanced electronic signature certificate under Article 33, Paragraph 2, Point 1.

Powers of the State Telecommunications Commission towards Registered Providers

Article 35

(1) The State Telecommunications Commission has the following powers:

1. registers the certification-service-providers;
2. refuses to register the certification-service-providers that do not fulfill the necessary requirements;
3. deletes the registration of the certification-service-providers.

(2) The State Telecommunications Commission shall provide information about the public keys of the registered certification-service-providers. The information is provided in an electronic form, contains the certificates and it is signed with the universal electronic signature of the State Telecommunications Commission.

Registration of the Certification-Service-Providers

Article 36

(1) Along with submitting an application for registration as a certification-service-provider the applicant shall present:

1. certificate for current court registration;
2. an insurance policy under article 21, paragraph 1, point 2;
3. the rules for issuance of a certificate, including the rules for ascertaining the identity of the owner of the universal electronic signature;
4. the security procedures applied during issuance and use of the universal electronic signature;
5. the terms and procedure for using the universal electronic signature, including the requirements for storing the private key;
6. the price for receiving and using a certificate as well as the prices for the rest of the services, provided by the certification-service-provider;
7. declaration that the requirements under Article 21, Paragraph 1, Points 1, 3 and 4 have been fulfilled;
8. documents proving the fulfillment of the requirements under Article 17 and Article 21, Paragraph 1, Points 5 - 8;

(2) The application for registration shall be considered in a one-month term. Registration may be denied only if the applicant has not presented the necessary documents, does not satisfy the requirements under Paragraph 1 of Article 21 and Article 17, or has not paid the necessary state fee.

(3) The notification for the denial should point all the defects of the application.

(4) The denial for registration shall be appealed through the procedure under the Law on Administrative Proceedings.

(5) The applicant may remove the defects and may submit a new application.

(6) The procedure for registration shall be specified with a Regulation of the Council of Ministers.

Deletion of Registration

Article 37

(1) The registration shall be deleted:

1. if the applicant has presented a false data;
2. in case of flagrant or systematic violations of this Law and of the Regulations on its application.

(2) The activities of the registered certification-service-provider shall be terminated with the deletion of the registration, unless the activities are not transformed to another registered certification-service-provider.

(3) The termination of the activities of the registered certification-service-providers on the issuance of the universal electronic signature certificates shall be regulated with the Regulation under Article 32, Paragraph 4.

Registry of Certification-Service-Providers

Article 38

(1) The registry of certification-service-providers shall be public. Anyone may request information for the registered certification-service-providers.

(2) Anyone may request information on the terms and procedure for registration of a certification-service-provider.

State Fees

Article 39

(1) For the registration of the certification-service-providers and providing information under Article 35, Paragraph 2 a state fee shall be collected.

(2) The rate of the state fee shall be specified with a tariff, approved by the Council of Ministers.

Activities of the Registered Certification-Service-Provider

Article 40

The registered certification-service-provider that has issued a certificate for universal electronic signature certifies the date and the hour of the presentation of the electronic document signed with such a signature.

Chapter five

APPLICATION OF ELECTRONIC DOCUMENT AND UNIVERSAL ELECTRONIC SIGNATURE BY THE STATE AND MUNICIPALITIES

Obligation for Accepting and Issuing Electronic Documents

Article 41

(1) The Council of Ministers shall determine its subordinate authorities, which:

1. may not deny acceptance of electronic documents, signed with an universal electronic signature;

2. may not deny issuance of permits, licenses, approvals, and other administrative acts in the form of an electronic document, signed with an universal electronic signature;

(2) The acceptance and issuance in the court system of electronic documents, signed with an universal electronic signature, shall be regulated by a Law.

(3) The acceptance and issuance of electronic documents, signed with an universal electronic signature, by other state authorities except for the ones under Paragraphs 1 and 2 and by the local self-government authorities shall be regulated by their own acts. The procedure and form for performing and storing of the electronic documents shall be regulated by internal rules.

Storage of Electronic Documents

Article 42

The state authorities and the local self-government authorities shall be obliged to store the electronic documents within the established period for storing documents.

Chapter six PROTECTION OF PERSONAL DATA

Obligation for Personal Data Protection

Article 43

(1) The protection of personal data, collected by the certification-service-providers, needed for the activities, carried out by them, and the protection of registers kept shall be regulated by a Law.

(2) The regime under Paragraph 1 shall also apply in relation to the personal data known to the State Telecommunications Commission, which during the performance of its obligations supervises the activities of the certification-service-providers.

(3) The certification-service-providers shall collect personal data about the signatory and the owner of the signature, only to the extent necessary for issuing and using a certificate.

(4) Data about a third party may be collected only with the explicit consent of the person it is related to.

(5) The collected data may not be used for purposes, different from the ones pointed in Paragraph 3, except with the explicit consent of the person it is related to or if this is permitted by a Law.

Chapter seven RECOGNITION OF CERTIFICATES ISSUED BY CERTIFICATION- SERVICE-PROVIDERS ESTABLISHED IN OTHER COUNTRIES

Grounds and Procedure

Article 44

(1) Certificates, issued by certification-service-providers, registered in other countries in accordance with the national legislation of these countries, shall be recognized as equal to certificates, issued by a Bulgarian certification-service-provider, if one of the following conditions has been met:

1. the obligations of the certification-service-provider that has issued the certificate and the requirements for its activities correspond to the requirements, provided in this Law, and the certification-service-provider is recognized in the country, where it is established;
2. a Bulgarian certification-service-provider that has been accredited by the organization under Article 20 or that has been registered under Article 34, has taken an obligation to be liable for actions or failure to take actions by the certification-service-provider, established in another country, in cases falling under Article 29; or
3. the certificate, or the certification-service-provider that has issued the certificate, were recognized according to an international agreement that has come into force.

(2) The conditions under Point 1 and 2 of Paragraph 1 shall be ascertained by the State Telecommunications Commission through the act of publishing into an electronic register of:

1. public key certificates of foreign certification-service-providers recognized by the State Telecommunications Commission to be in conformity with Paragraph 1, Point 1.
2. the electronic signature certificate of the foreign certification-service-

provider, for which the liability has been accepted under Paragraph 1, Point 2 and the electronic signature certificate of the Bulgarian certification-service-provider that has accepted the liability and conditions upon which the liability has been accepted.

Chapter eight ADMINISTRATIVE PENAL PROVISIONS

Penalties

Article 45

(1) Anyone who commits or allows the commitment of an offence under Article 17, Article 18, Article 19, Paragraph 1, Article 21, Paragraphs 1 and 3, Article 22, Article 24, Paragraphs 1 and 2, Article 25, Paragraphs 2, 3 and 5, Article 26, Paragraphs 2, 3, 4, 5 and 6, Article 27, Paragraphs 2 and 3, Article 28, Paragraph 1, 2 and 3, Article 29, Paragraph 1, Article 30, Paragraph 1 shall be liable to a fine from 100 to 10 000 BGL, if the offence is not qualified as a crime.

(2) In cases under Paragraph 1 a legal person or a sole proprietor shall be liable to a property sanction to an amount from 500 to 50 000 BGL.

Findings of the Offences, Drawing up of Statements and Issuance of Penal Enactments

Article 46

(1) The statements on findings of the offences shall be drawn up by persons, authorized by the Chair of the State Telecommunications Commission and the penal enactments shall be issued by him or her or by an official, authorized by him or her.

(2) With the finding of the offences persons drawing up the statements may confiscate and retain the material evidence related to the ascertaining of the offences through the procedure under Article 41 of the Law on Administrative Offences and Penalties.

(3) The drawing up of statements and the issuance, appeal, and execution of penal enactments shall be carried out through a procedure set up in the Law on Administrative Offences and Penalties.

SUPPLEMENTARY PROVISION

§ 1. Within the meaning of this Law:

1. 'Qualified written form' is a form for validity or form giving proof, where the law envisages additional requirements to the written form, such as certification of a signature by a notary, deed of a notary, handwritten statement, participation of witnesses or civil servants at the time the statement was performed and others.

2. 'Asymmetric cryptosystem' shall be a system for encryption of information, allowing the creation and use of cryptographic key pairs, that includes a private key connected through an algorithm to a public key, and having the following characteristics:

a) the content of the electronic statement can be encrypted with one of the keys, and it can be decrypted with the other;

b) through the use of the public key it can be undoubtedly determined whether

the transformation of the original electronic statement has been made using its corresponding private key and whether the electronic statement has been altered after its transformation;

c) if one of the keys is made known, it is practically impossible to find out the other.

3. 'Cryptographic key' shall be a sequence of bits, used in an algorithm for the transformation of information from readable into ciphered form (encryption) or vice versa from ciphered into readable form (decryption).

4. 'Public key' shall be the one of the key pair, used in an asymmetric cryptosystem, that is accessible to all and used by everyone for the electronic signature verification;

5. 'Private key' shall be the one of the key pair, used in an asymmetric cryptosystem for the electronic signature creation;

6. 'Signature-creation-device' shall be the configured software or hardware used to implement the signature-creation-data;

7. 'Signature-creation-data' shall be the unique data such as codes or cryptographic keys, used by the signatory for an electronic signature creation.

TRANSITIONAL AND FINAL PROVISIONS

§2. In the Law on Telecommunications (Promulgated: SG 93/August 11, 1998; Amended: SG 26/March 23, 1999, in force since March 23, 1999; SG 10/February 4, 2000, in force since February 4, 2000; SG 64/August 4, 2000) in Article 22 a new paragraph 4 is added:

"**(4)** The State Telecommunications Commission registers and supervises provision of certification services, related to electronic signatures, under the procedure set up in a separate law."

§3. This Act comes into force six months after its promulgation in State Gazette.

§4. The Council of Ministers shall prepare the Regulations referred to in this Law within a period of five months after its promulgation and shall adopt them in one-month term after the Law comes into force.

§5. The application of this Law is assigned to the Council of Ministers and to the State Telecommunications Commission.

The Act was adopted by the XXXVIII National Assembly on March 22, 2000, and affixed with State Seal.

For the Chairman of the National Assembly:

(Mr. Yordan Sokolov)