Digital Signatures Act

Passed 8 March 2000

(RT[1] I 2000, 26, 150),
entered into force 15 December 2000,
amended by the following Acts:
4.12.2008 entered into force 12.01.2009 - RT I 2009, 1, 3
15.02.2007 entered into force 1.01.2008 - RT I 2007, 24, 127
24.01.2007 entered into force 1.01.2008 - RT I 2007, 12, 66
17.12.2003 entered into force 08.01.2004 - RT I 2003, 88, 594
17.12.2003 entered into force 01.01.2004 - RT I 2003, 88, 591
19.06.2002 entered into force 01.08.2002 - RT I 2002, 61, 375
05.06.2002 entered into force 01.07.2002 - RT I 2002, 53, 336
12.06.2001 entered into force 07.07.2001 - RT I 2001, 56, 338
15.11.2000 entered into force 01.01.2001 - RT I 2000, 92, 597

Chapter I
General Provisions

§ 1. Scope of application of Act

This Act provides the necessary conditions for using digital signatures and digital seals, and the procedure for exercising supervision over the provision of certification services and time-stamping services.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

§ 2. Digital signature

(1) A digital signature is a data unit, created using a system of technical and organisational means, which a signatory uses to indicate his or her connection to a document.
(2) A digital signature is created by using the data necessary for giving a signature contained in a safe signature creating device (hereinafter private key) to which the data needed for verification of the signature contained in a signature verification device (hereinafter public key) uniquely corresponds.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)
(3) A digital signature and the system of using the digital signature shall:

1) enable unique identification of the person in whose name the signature is given;
2) enable determination of the time at which the signature is given;
3) link the digital signature to data in such a manner that any subsequent change of the data or the meaning thereof is detectable.

§ 2^1. Digital seal
(1) A digital seal is a body of data created by a system of technical and organisational means which the holder of the digital seal certificate uses to certify the integrity of a document and to link the holder of the certificate to such document.
(2) A digital seal is created by a private key contained in a safe signature creating device to which the public key uniquely corresponds.
(3) A digital signature and the system of using the digital signature shall:
1) enable unique identification of the holder of the certificate in whose name the signature is given;
2) enable determination of the time at which the digital seal is given;
3) link the digital seal to the data in the document in such a manner that any subsequent change of the data or the meaning thereof is detectable.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

§ 3. Legal consequences of digital signatures
(1) A digital signature has the same legal consequences as a hand-written signature if these consequences are not restricted by law and if the compliance of the signature with the requirements of subsection 2 (3) of this Act is proved.
(2) The compliance of a digital signature given according to the principles provided for in Chapters II-V of this Act with the requirements of subsection 2 (3) of this Act need not be proved separately if data and the digital signature enable unique determination of the certificate which contains the public key to which the private key with which the digital signature is given corresponds.
(3) A digital signature does not have the consequences provided for in subsection (1) of this section if it is proved that the private key was used for giving the signature without the consent of the holder of the corresponding certificate.
(4) The giving of a digital signature without the consent of the holder of the corresponding certificate is deemed to be proved if the certificate holder proves circumstances which existed and due to which it may be presumed that the signature was given without his or her consent.

(5) In the cases specified in subsection (3) of this section, the certificate holder shall compensate damage caused to another person who erroneously presumed that the signature was given by the certificate holder, if the private key was used without the consent of the certificate holder due to the intent or gross negligence of the certificate holder.

§ 4. Use of digital signatures and digital seals
State and local government agencies, legal persons in public law, and persons in private law performing public law functions are required to provide access through the public data communication network to information concerning the possibilities and procedure for using digital signatures and digital seals in communication with such agencies and persons.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

§ 4^1. Application of Administrative Procedure Act
The provisions of the Administrative Procedure Act (RT I 2001, 58, 354; 2002, 53, 336) apply to administrative proceedings prescribed in this Act, taking account of the specifications provided for in this Act.
(19.06.2002 entered into force 01.08.2002 - RT I 2002, 61, 375)

Chapter II
Certificates

Division 1
Certificates and Requirements for Certificates

§ 5. Certificates
(1) For the purposes of this Act, a certificate is a document which is issued in order to enable a digital signature or digital seal to be given and verified and in which a public key is uniquely linked to the holder of the certificate.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)
(1^1) Several digital seal certificates may be issued to one person.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)
(2) A certificate shall set out:
1) the number of the certificate;

2) the name of the holder of the certificate;

2[1]) the personal identification or registry code of the certificate holder;

(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

3) the public key of the certificate holder;

4) the period of validity of the certificate;

5) the issuer and registry code of the issuer;

6) a description of the limitations on the scope of use of the certificate.

(3) The issuer of a certificate shall confirm each certificate issued thereby.

§ 6. Certificate holder

For the purposes of this Act, a certificate holder is a natural person in the case of a digital signature and either a natural or a legal person in the case of a digital seal, to whose personal data the public key contained in the certificate is linked in the same certificate.

(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

Division 2

Application for and Issue of Certificates

§ 7. Creation of private and public keys

(1) A private key and a public key shall be created by an applicant for a certificate or, at his or her request and according to an agreement between the parties, by a certification service provider or another person or agency.

(2) Persons who create private and public keys for other persons shall not create copies of the keys for themselves or for third parties.

§ 8. Application for certificates

(1) A person wishing to obtain a certificate for giving and verifying a digital signature shall submit a written application to a certification service provider setting out:

(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

1) the given name and surname of the applicant for the certificate;

2) the personal identification code of the applicant for the certificate or, in the absence of a personal identification code, the day, month and year of birth of the applicant for the certificate;

3) the public key of the applicant for the certificate if it exists or an authorisation

to the certification service provider for the creation of a private and public key;
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

4) the contact details of the applicant for the certificate;

5) the period of validity of the certificate applied for;

6) a description of the limitations on the scope of use of the certificate;

7) other data which the applicant applies to have added to the certificate.

(1^1) A person wishing to obtain a certificate for giving and verifying a digital seal shall submit a written application to a certification service provider setting out:

1) the name of the applicant for the certificate;

2) the personal identification code or the registry code and seat or residence of the applicant for the certificate;

3) the public key of the applicant for the certificate or an application for the creation of a private and public key by the certification service provider;

4) the contact details of the applicant for the certificate;

5) the period of validity of the certificate applied for;

6) other data which the applicant applies to have added to the certificate.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

(2) If the public key of an applicant for a certificate is set out in an application specified in subsection (1) or (1^1) of this section, the applicant for the certificate shall prove that the private key corresponding to the public key is in his or her possession.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

§ 9. Issuer of certificates

For the purposes of this Act, an issuer of a certificate is a person or agency who issues the certificate and is responsible for the accuracy of the data contained in the certificate.

§ 10. Issue of certificates

(1) The issuer of a certificate is required to verify that the application submitted in order to apply for the certificate complies with this Act and that the data contained in the application is accurate.

(1^1) The issuer of a certificate has the right to verify the validity of an identity document used for checking the identity of (identifying) a person and the right of representation of a person.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

(2) A certificate shall be issued to a person promptly after entry of the corresponding data in the database of certificates which is maintained by the issuer of the certificate.
(3) The issuer of a certificate is required to notify the applicant for the certificate of the conditions of use of the certificate, the rights and obligations of the certificate holder, and other circumstances related to the use of the certificate.

Division 3
Period of Validity, and Suspension and Revocation of Certificates

§ 11. Period of validity of certificates
(1) A certificate is valid as of the beginning of the period of validity set out in the certificate but not before entry of the corresponding data in the database of certificates which is maintained by the issuer of the certificate.
(2) A certificate expires upon expiry of the period of validity set out in the certificate or upon revocation of the certificate.

§ 12. Suspension of certificates
(1) A certification service provider has the right to suspend a certificate if the certification service provider has a justified reason to believe that incorrect data has been entered in the certificate or that it is possible to use the private key corresponding to the public key contained in the certificate without the consent of the certificate holder.
(2) A certification service provider is required to suspend a certificate if this is requested by:
1) the certificate holder;
2) the data protection supervision authority or the chief processor of the register of certificates if there is a justified reason to believe that incorrect data has been entered in the certificate or that it is possible to use the private key corresponding to the public key contained in the certificate without the consent of the certificate holder;
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)
3) a court, prosecutor’s office or agency which conducts pre-trial investigations in criminal matters in order to combat criminal offences.
(3) After verification of the legality of the claim for suspension of a certificate, the certification service provider is required to promptly enter the data concerning suspension in the database of certificates which is maintained thereby.

(4) The certification service provider shall notify the certificate holder promptly of suspension of a certificate.
(5) Certification service providers are required to maintain records of the time of and bases and applicants for suspension of certificates, and of termination of the suspension of certificates.
(6) Digital signatures or digital seals given during the period when the certificate is suspended are invalid.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

§ 13. Termination of suspension of certificates
(1) Suspension of a certificate shall be terminated on the basis of an application by the certificate holder or a person or agency which requests the suspension of the certificate by entry of the corresponding data in the database of certificates which is maintained by the certification service provider which issued the certificate.
(2) In the cases specified in clause 12 (2) 3) of this Act, the person who initiates the suspension may terminate the suspension of a certificate.
(3) A certification service provider shall notify the certificate holder promptly of termination of the suspension of the certificate.

§ 14. Revocation of certificates
(1) The following are the bases for revocation of a certificate:
1) an application by the certificate holder;
2) the opportunity for the private key corresponding to the public key set out in the certificate to be used without the consent of the certificate holder;
3) divestment of the certificate holder of active legal capacity;
4) declaration of the certificate holder as dead;
5) the death of the certificate holder;
5^1) deletion from the register of the certificate holder due to dissolution or release or removal from office of a certificate holder who is a holder of office in public law;
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)
6) submission of false data to a certification service provider by the certificate holder in order to obtain the certificate;
7) termination of the activities of the certification service provider;
8) other cases provided by law.
(2) Certificate holders or other persons have the right to request revocation of a certificate by submission of a corresponding application.

(3) A certificate shall be revoked by a certification service provider who initiates proceedings for revocation promptly after receipt of a corresponding application or upon the existence of another basis provided for in subsection (1) of this section.

§ 15. Proceedings for revocation of certificates

(1) If the cases set out in clauses 14 (1) 3)-8) of this Act are the reasons for revocation of a certificate, the documents which certify the basis for revocation of the certificate shall be appended to the application.

(2) Certification service providers are required to verify the legality of applications and the bases for revocation of certificates.

(3) A certificate expires as of entry of the corresponding data in the database of certificates which is maintained by the certification service provider.

(4) Certification service providers are required to preserve documents which certify the reasons for revocation of a certificate until the termination of their activities, unless another term is provided for by law.

§ 16. Consequences of suspension and revocation of certificates without legal basis

A person or agency who, without legal basis, intentionally or due to gross negligence causes suspension or revocation of a certificate is required to compensate damage caused by the suspension or revocation of the certificate.

Chapter III

Certification Services and Certification Service Providers

§ 17. Certification services

(1) The issue of certificates necessary for giving digital signatures and digital seals, the enabling of verification of digital signatures and digital seals given on the basis of such certificates, and proceedings for suspension, termination of suspension and revocation of such certificates are certification services.

(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

(2) Certification is an act as a result of which a certification service provider issues a certificate to an applicant for a certificate.

§ 18. Certification service providers

(1) The following agencies and persons which are entered in the register of certificates as service providers and which are registered in the corresponding register

in Estonia may be certification service providers:
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)
1) public limited companies;
2) private limited companies the share capital of which exceeds 400 000 kroons;
3) legal persons in public law if this is prescribed in an Act concerning the legal person in public law;
4) state agencies determined by the Government of the Republic.
(2) (Repealed - 06.06.2001 entered into force 07.07.2001 - RT I 2001, 56, 338)

§ 19. Requirements for certification service providers
(1) Certification service providers shall comply with the requirements established by this Act and be capable of ensuring reliable certification services in accordance with Acts and legislation issued on the basis of Acts.
(2) Certification service providers are required to ensure the conduct of an annual information systems audit by the date of entry in the register of certificates, and to submit the results of the audit to the authorised processor of the register of certificates.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)
(3) Certification service providers shall not have tax arrears or other arrears which endanger the provision of certification services in compliance with the principles provided for in Chapters II-V of this Act.
(4) Certification service providers are required to insure their activities pursuant to the procedure provided for in § 39 of this Act.

§ 20. Certification principles
(1) The descriptions of the organisational and technical means which comply with this Act and requirements established on the basis thereof and which are used in certification by certification service providers, and the descriptions of the requirements set for applicants for certificates by certification service providers are certification principles.
(2) The certification principles of a certification service provider shall set out the following:
1) the name of the certification service provider;
2) the address of the seat of the certification service provider;
3) the procedure for proving the private key corresponding to the public key of the applicant for the certificate;
4) a description of the technical means used to provide certification services;

5) the procedure and terms for certification proceedings;
6) the procedure for review of applications for certificates;
7) the procedure for issue of certificates;
8) the mechanisms for description of limitations on the scope of use of certificates;
9) the procedure for maintaining records of the issued certificates;
10) the procedure for release of information concerning the validity of certificates;
11) the procedure for generation and storage of keys and the description of the means prescribed for the storage of the personal key of the certification service provider;
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)
11^1) the procedure for confirmation of the issued certificates;
12) the procedure for suspension and revocation of certificates;
13) an action plan in case it is possible to imitate the certification service provider or the activities thereof upon provision of services;
14) the technical procedure for suspension, termination of suspension, and revocation of certificates issued by the certification service provider;
15) the procedure for termination of the provision of certification services;
16) other circumstances which the certification service provider deems necessary to have provided in the certification principles.
(3) The certification principles of a state agency which is determined by the Government of the Republic and which provides certification services, and the cost of the services provided by the state agency shall be approved by the head of the state agency.

§ 21. Restrictions on employees of certification service providers
Employees of certification service providers who are involved in providing certification services shall not have a criminal record for an intentionally committed criminal offence.

§ 22. Duties of certification service providers
Certification service providers are required to:
1) publicise their certification principles and ensure accessibility thereto in the public data communication network;
2) ensure maintenance of the confidentiality of information not subject to disclosure which becomes known thereto upon the provision of certification services;

3) maintain records of the certificates issued thereby and the validity thereof;
4) accept applications for the suspension of certificates twenty-four hours a day;
5) certify, at the request of an interested person, by the digital signature of a representative thereof the validity of a digital signature given by a private key corresponding to the public key contained in a certificate issued thereby;
6) ensure that it is possible to verify the validity of certificates in the public data communication network twenty-four hours a day;
7) preserve documentation related to certification until the termination of their activities;
8) ensure the conduct of an annual information systems audit and submit the results of the audit to the authorised processor of the register of certificates;
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)
9) publicise the conditions of compulsory insurance contracts in the public data communication network;
10) inform the authorised processor of the register of certificates of any changes to a public key used for the provision of certification services.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

Chapter IV
Time-stamping Services and Time-stamping Service Providers

§ 23. Definition of time stamp

(1) A time stamp is a data unit which is created using a system of technical and organisational means which certifies the existence of a document at a given time.
(2) A time stamp shall be linked to data in such a manner as to preclude the possibility of changing the data undetectably after obtaining a time stamp.
(3) Time-stamping service providers shall confirm the time stamps issued thereby.

§ 24. Time-stamping services

(1) Time-stamping services are the issue of time stamps necessary to prove the official time and temporal order of digital signatures and digital seals and the creation of conditions for verification of issued time stamps.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)
(2) If it is impossible to determine the official time and temporal order of time stamps issued by different time-stamping service providers, the time stamps are deemed to have been issued simultaneously.

(3) Time-stamping service providers shall ensure that it is impossible to issue a correct time stamp for a time earlier or later than application therefor or change the order in which time stamps are issued.

§ 25. Time-stamping service providers

The following persons and agencies which are entered in the register of certificates as corresponding service providers and which are registered in the corresponding register in Estonia may be time-stamping service providers:

(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

1) public limited companies;

2) private limited companies the share capital of which exceeds 400 000 kroons;

3) legal persons in public law if this is prescribed in an Act concerning the legal person in public law;

4) state agencies determined by the Government of the Republic.

§ 26. Requirements for time-stamping service providers

(1) Time-stamping service providers shall comply with the requirements established by this Act and be capable of ensuring reliable time-stamping services in accordance with Acts and legislation issued on the basis of Acts.

(2) Time-stamping service providers are required to ensure the conduct of an annual information systems audit by the date of entry in the register of certificates, and to submit the results of the audit to the authorised processor of the state register of certificates.

(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

(3) Time-stamping service providers shall not have tax arrears or other arrears which endanger the provision of time-stamping services in compliance with the principles provided for in Chapters II-V of this Act.

(4) Time-stamping service providers are required to insure their activities pursuant to the procedure provided for in § 39 of this Act.

§ 27. Time-stamping principles

(1) The descriptions of operations performed in order to issue and verify time stamps and the descriptions of the technical means used by the time-stamping service providers are time-stamping principles.

(2) The time-stamping principles of a time-stamping service provider shall set out the following:

1) the name of the time-stamping service provider;
2) a description of the technical means used to provide time-stamping services;
3) the procedure for obtaining and verifying time stamps;
3^1) the procedure for confirmation of the issued time stamps;
4) the procedure for maintaining records of the issued time stamps;
5) the procedure for release of information concerning the issued time stamps;
6) the procedure for termination of the provision of time-stamping services;
7) an action plan in case it is possible to imitate the time-stamping service provider or the activities thereof upon provision of services;
8) other circumstances which the time-stamping service provider deems necessary.

§ 28. Duties of time-stamping service providers
Time-stamping service providers are required to:
1) ensure correct indications of time on time stamps pursuant to the descriptions provided in the time-stamping principles;
2) maintain records of issued time stamps;
3) preserve documentation in order to verify issued time stamps;
4) (Repealed 4.12.2008 – entered into force 12.01.09 - RT I 2009, 1, 3)
5) ensure that it is possible to obtain and verify time stamps in the public data communication network;
6) ensure the conduct of an annual information systems audit and submit the results of the audit to the authorised processor of the register of certificates;
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)
7) publicise the conditions of compulsory insurance contracts in the public data communication network.
8) inform the authorised processor of the register of certificates of any changes to a public key used for the provision of time-stamping services.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

§ 29. Restrictions on employees of time-stamping service providers
Employees of time-stamping service providers who are involved in providing certification services shall not have a criminal record for an intentionally committed criminal offence.

Chapter V

Termination of Provision of Certification Services and Time-stamping Services

§ 30. Termination of provision of certification services and time-stamping services

(1) The provision of certification services and time-stamping services (hereinafter services) shall be terminated:

1) by a decision of the service provider;

2) by a decision of the agency exercising supervision over the provision of services;

3) by a court judgment;

4) upon liquidation of the service provider or termination of the activities thereof;

5) by a Government of the Republic resolution which terminates the provision of services by state agencies specified in clauses 18 (1) 4) and 25 4) of this Act.

(2) Upon termination of the provision of certification services and time-stamping services, the service provider shall transfer documentation concerning provision of the service to the register of certificates.

(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

§ 31. Notification of termination of provision of services

(1) A service provider is required to notify the authorised processor or the chief processor of the register of certificates promptly of a decision to terminate provision of the service. If the person or agency notifies the authorised processor of the register of the decision to terminate the provision of services, the authorised processor is required to notify the chief processor of the register thereof promptly.

(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

(2) A service provider is required to notify users of the service thereof of a decision to terminate provision of the service at least one month before termination of provision of the service.

(3) The chief processor of the register of certificates shall notify the data protection supervision authority and the state information systems co-ordination authority of any decision to terminate provision of a service.

(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

Chapter VI

Register of Certificates

(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

§ 32. Register of certificates

(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

(1) The register of certificates (hereinafter register) is a database established by the Government of the Republic which is established and introduced in order to maintain records of certification service providers and time-stamping service providers.

(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

(2) The chief processor of the register is the Ministry of Economic Affairs and Communications.

(3) The register comprises:

1) a database of certification service providers;

2) a database of time-stamping service providers;

3) (Repealed 4.12.2008 – entered into force 12.01.09 - RT I 2009, 1, 3)

4) the registry archives.

§ 33. Application for entry of service providers in register

(1) In order to be registered in a register, a person or agency shall submit the following:

1) an application for registration of the person or agency as a service provider, which is signed by a legal representative and which sets out the public key (public keys) which the person or agency will begin to use upon the provision of certification services or time-stamping services by the person or agency;

2) the same application in digital form, which is certified pursuant to the procedure for certification of the issued certificates and time stamps and which includes proof concerning possession of private keys used upon provision of certification services or time-stamping services;

3) (Repealed - 19.06.2002 entered into force 01.08.2002 - RT I 2002, 61, 375)

4) the certification or time-stamping principles;

5) (Repealed - 19.06.2002 entered into force 01.08.2002 - RT I 2002, 61, 375)

6) the results of the information systems audit;

7) confirmation concerning the absence of arrears which endanger the provision of services in compliance with the principles provided for in Chapters II-V of this Act.

(2) An application for the entry of a service provider in the register shall set out the following:

1) the name of the service provider;

2) the address of the seat of the service provider;

3) the registry code of the service provider;

4) the name, title, personal identification code and contact details of the representative of the service provider;

5) the telecommunications numbers and addresses of the service provider;

6) the limitations established on provision of the service.

(3) The authorised processor of the register is required to verify the accuracy of the submitted data and the compliance of the service with the requirements of this Act. Additionally, the authorised processor of the register shall verify whether the applicant has paid the state fee, whether the person or agency which provides the service is registered and whether the person owes tax arrears to the Tax and Customs Board.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

(4) The authorised processor of the register has the right to make inquiries to all state agencies and state and local government databases in order to verify the accuracy of the data submitted by a person or agency.

(5) Before entry in the register, a person or agency is required to ensure the conduct of an information systems audit, the results of which shall be submitted to the authorised processor of the register. The cost of the information systems audit shall be borne by the person or agency.
(17.12.2003 entered into force 08.01.2004 - RT I 2003, 88, 594)

§ 34. Registration of service providers

(1) After verification of the documents, the authorised processor of the register shall decide on the registration of a person or agency in the register as a service provider within five working days after the date of receipt of the documents and data specified in subsections 33 (1) and (2) of this Act and shall communicate the decision to the person or agency.

(2) If the term provided for in subsection (1) of this section is not sufficient for verification of the submitted data and documents, the chief processor of the register may extend the term up to ten working days.

(3) After a decision is made to register a person or agency in the register, the person or agency shall submit a copy of an insurance policy which complies with the requirements of § 39 of this Act to the authorised processor after which the person or agency shall promptly be registered as a service provider.

(4) The authorised processor of the register shall grant a non-recurrent registry code to each service provider entered in the register.

(5) The authorised processor of the register shall approve the public keys of registered service providers set out in clause 33 (1) 1) of this Act.

(6) Upon termination of the provision of a service, a corresponding application shall be submitted to the authorised processor of the register who shall input data on the termination of provision of the service in the register.
(19.06.2002 entered into force 01.08.2002 - RT I 2002, 61, 375)

§ 35. Refusal to register service providers

(1) The authorised processor of the register shall refuse to register a service provider:

1) if the person or agency does not comply with the requirements provided for in this Act;

2) if the certification or time-stamping principles are not in compliance with the requirements provided for in this Act;

3) (Repealed - 19.06.2002 entered into force 01.08.2002 - RT I 2002, 61, 375)

4) if the person or agency submits incorrect data to the authorised processor of the register;

5) if, on the basis of the submitted results of the information systems audit, there is reason to believe that the person or agency is unable to ensure services which are in compliance with the requirements of this Act;

6) if the person or agency has tax arrears, is not registered or has not paid the state fee;

7) in other cases provided by law.

(2) The authorised processor of the register shall deliver a decision on refusal to register a service provider to the person or agency by post or by electronic means.
(19.06.2002 entered into force 01.08.2002 - RT I 2002, 61, 375)

§ 36. Deletion of service providers from register

A service provider shall be deleted from the register if the service provider has terminated the provision of services pursuant to the provisions of Chapter V of this Act.

§ 37. Access to registered data

(1) Data entered in the register are public.

(2) The authorised processor of the register is required to ensure access to the data stored in the register concerning service providers, and the availability thereof twenty-four hours a day.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

Chapter VI[1]
Secure Signature-creation Devices
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

§ 371. Requirements for secure signature-creation devices
(1) A secure signature-creation device is an adapted piece of software or hardware, for example a microchip card equipped with a security chip, which is used for the storage and application of a personal key.
(2) Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
1) the personal key used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
2) the personal key cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
3) the personal key used for signature generation can be reliably protected by the legitimate signatory against the use of others can appropriately protect the personal key such that other persons will not be able to use it.
(3) Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

Chapter VII
Proprietary Liability of Service Providers and Insurance

§ 38. Proprietary liability of service providers
(1) Service providers are liable for patrimonial damage which is caused as a result of violation of the obligations of the service provider.
(2) If a third person besides the service provider is liable for loss specified in subsection (1) of this section, they shall be solidarily liable.
(5.06.2002 entered into force 1.07.2002 - RT I 2002, 53, 336)

§ 39. Compulsory insurance of service providers
(1) In order to ensure compensation for loss provided for in § 38 of this Act, service providers are required to enter into compulsory insurance contracts.
(2) Service providers are required to publicise the conditions of insurance contracts in the public data communication network.

Chapter VIII
Recognition of Certificates Issued by Foreign Certification Service Providers and of Digital Signatures and Digital Seals Created on Basis thereof
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

§ 40. Recognition of foreign certificates
Certificates issued by a foreign certification service provider shall be recognised as equivalent to certificates issued by certification service providers acting on the basis of this Act if at least one of the following conditions is met:

1) according to the decision of the chief processor of the register, the foreign certification service provider complies with the requirements provided for in this Act and legislation established on the basis thereof;

2) the certificates of the foreign certification provider are guaranteed by a certification service provider acting on the basis of this Act who assumes responsibility for the accuracy of the data contained in the certificates;

3) the certificates issued by the foreign certification service provider are recognised by an international agreement entered into by the Republic of Estonia.

Chapter IX
Supervision of Certification Service Providers and Time-stamping Service Providers

§ 41. Supervisory authorities
(1) The Ministry of Economic Affairs and Communications shall monitor observance of the requirements of this Act and legislation established on the basis thereof.

(2) The chief processor of the register shall exercise supervision over the maintenance of the register pursuant to the procedure prescribed in the Public Information Act.
(24.01.2007 entered into force 1.01.2008 - RT I 2007, 12, 66)

(3) The data protection supervision authority shall exercise supervision over the legality of maintenance of the register and over the protection of data pursuant to the procedure prescribed in the Public Information Act and the Personal Data Protection Act.
(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

§ 42. Exercise of supervision

The Ministry of Economic Affairs and Communications, as the agency which monitors observance of the requirements of this Act and legislation established on the basis thereof, has the right to:

(17.12.2003 entered into force 08.01.2004 - RT I 2003, 88, 594)

1) verify the accuracy of results of the information systems audit submitted to the register;

2) enter premises which are used for the provision of services and examine documents concerning the provision of services in the presence of a representative of the service provider;

3) make inquiries to all state agencies and state and local government databases in order to obtain corresponding data;

4) issue a written caution to a service provider if the service provider fails, for the first time or due to negligence, to comply with the requirements of this Act or legislation issued on the basis thereof;

5) issue a precept for a specified term to a service provider if the service provider does not respond to a caution specified in clause 4) of this section or fails repeatedly or intentionally to implement this Act or observe legislation issued on the basis thereof;

6) impose penalty payments in the amount of up to 50 000 kroons pursuant to the procedure provided in the Substitute Enforcement and Penalty Payment Act upon failure to comply with a precept specified in clause 5) of this section;

(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)

7) decide on the deletion of a service provider from the register and submit the decision to the authorised processor of the register in order for a corresponding entry to be made.

Chapter X

Implementing Provisions

§ 43. Implementation of digital signatures

(1) The Government of the Republic shall establish and introduce the register provided for in subsection 32 (1) of this Act by the time this Act enters into force.

(2) The Government of the Republic shall establish uniform bases for the document management procedures of state and local government agencies and legal persons in public law by 1 March 2001 and the bases shall also enable the use of digitally signed documents in the document management of the agencies.

(3) State and local government agencies and legal persons in public law shall reorganise the document management thereof pursuant to the document management procedures provided for in subsection (2) of this section by 1 June 2001.
(4) The Minister of Economic Affairs and Communications shall approve the procedure for the information systems audit of service providers by 1 October 2000.
(17.12.2003 entered into force 08.01.2004 - RT I 2003, 88, 594)

§ 44. Approval of use of public keys of authorised processor of register and service providers and determination of scope of use of private keys corresponding thereto
(1) The Minister of Economic Affairs and Communications shall approve the public key of the authorised processor of the register, which is used for the approval of the public keys of certification service providers and time-stamping service providers set out in clause 33 (1) 1) of this Act, and shall determine the scope of use of the private key corresponding thereto.
(2) The authorised processor of the register shall approve the public key used for the provision of certification services or time-stamping services by certification service providers and time-stamping service providers, and the scope of use of the private key corresponding thereto.
(17.12.2003 entered into force 08.01.2004 - RT I 2003, 88, 594)

§ 45. Amendment of State Fees Act
The State Fees Act (RT I 1997, 80, 1344; 2001, 55, 331; 56, 332; 64, 367; 65, 377; 85, 512; 88, 531; 91, 543; 93, 565; 2002, 1, 1; 9, 45; 13, 78; 79; 81; 18, 97; 23, 131; 24, 135; 27, 151; 153; 30, 178; 35, 214; 44, 281; 47, 297; 51, 316; 57, 358; 58, 361; 61, 375) is amended as follows:

1) clause 26^3) is added to subsection 3 (2) worded as follows:

«26^3) acts performed on the basis of the Digital Signatures Act;"

2) Division 18^2 is added to Chapter 7 of the Act worded as follows:

“Division 18^2

Acts Performed on Basis of Digital Signatures Act

§ 186^3. Making and amendment of entries concerning certification service providers and time-stamping service providers in state register of certificates
(1) A state fee of 10 000 kroons shall be paid for registration of a certification service provider or a time-stamping service provider in the state register of certificates.
(2) A state fee of 100 kroons shall be paid for entry of amendments to data

concerning a certification service provider or a time-stamping service provider in the state register of certificates.

§ 46. Amendment of Identity Documents Act

The Identity Documents Act (RT I 1999, 25, 365; 2000, 25, 148; 26, 150; 40, 254; 86, 550; 2001, 16, 68; 31, 173; 56, 338; 2002, 61, 375) is amended as follows:

1) subsection (5) is added to § 9 worded as follows:

«(5) Information which enables digital identification and signing and other digital data, the list of which shall be established by a regulation of the Government of the Republic, may be entered in a document.”;

2) subsection (6) is added to § 15 worded as follows:

«(6) The issuer of a document shall identify the person applying for the document. The procedure for identification shall be established by a regulation of the Minister of Internal Affairs.

§ 47. Entry into force of Act

This Act enters into force on 15 December 2000.

_____

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.01.2000, pp 12–20)

(4.12.2008 entered into force 12.01.09 - RT I 2009, 1, 3)