Act XXXV of 2001

on Electronic Signatures

Understanding and embracing the direction of overall progress of the information society - for it represents one of the most important developments of the new millennium -Parliament adopts this Act on electronic signatures to ensure adequate background for the legal recognition of authentic electronic statements and electronic communication in commerce, administration and other aspects of life affected by the information society.

Scope, Principles, Derogations and Definitions

Section 1.

(1) This Act shall apply

a) to all natural and legal persons, other entities and organizations who provide services related to electronic signatures;

b) to all natural and legal persons, other entities and organizations using electronic signatures and services related to electronic signatures;

c) to services related to electronic signatures and to certain matters concerning the use of electronic signatures.

(2) The conditions for accepting electronic documents by organizations (persons) under restricted and closed systems - within the limitations defined in Subsection (2) of Section 3 - may be stipulated by parties under contract by way of derogation from the provisions of this Act, for which Subsection (1) of Section 3 shall apply regardless.

(3) With the exceptions laid down in Point 6. of Section 2 and Subsection (1) of Section 3, this Act shall not apply to electronic signatures which are not recognized as advanced electronic signatures.

Section 2.

For the purposes of legal regulations the following definitions shall apply:

1) 'Signature-creation data' shall mean unique data, such as private cryptographic keys, which are used by the signatory to create an electronic signature.

2) 'Signature-verification-data' shall mean unique data, such as public cryptographic keys, which are used for the purpose of verifying an electronic signature on an electronic communication or electronic document.

3) 'Signature-creation device' shall mean configured software or hardware used by a signatory to produce an electronic signature by implementing the signature-creation data.

4) 'Signatory' shall mean a natural person to whom specific signature-verification data is linked according to the directory of signature-verification data published by an electronic signature certification-service-provider (hereinafter referred to as "certification-service-provider")

5) 'Secure-signature-creation device' shall mean a signature-creation device which meets the requirements laid down in Schedule No. 1 to this Act.

6) 'Electronic signature' shall mean data or document in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

7) 'Signature verification process' shall mean a process to ensure that the data used for verifying the signature on an electronic document corresponds to the data displayed, and to establish the

signatory's identity using the data on the document and the signature-verification-data published by a certification-service-provider and the certificate.

8) 'Application of electronic signature' shall mean when an electronic signature is affixed to electronic data, and the verification of an electronic signature.

9) 'Electronic signature certification-service-provider' shall mean a person (organization) who is engaged in the activities defined in Subsection (2) of Section 6.

10) 'Electronic signing' shall mean when an electronic signature is attached to or logically associated with electronic data.

11) 'Electronic-signature product' shall mean hardware or software, or relevant components thereof, which are intended to be used for the provision of electronic-signature services, such as the creation or verification of electronic signatures or time-stamps.

12) 'Electronic document' shall mean data processed by electronic means and which contains an electronic signature.

13) 'Electronic communication' shall mean an electronic document whose purpose is to communicate a written text and which contains any other data solely if such data are closely associated with the text, i.e. for identification (e.g. header) or for better understanding (e.g. chart).

14) 'Electronic statement' shall mean an electronic communication which contains a declaration or approval of a declaration, or a commitment to abide by a declaration.

15) 'Advanced electronic signature' shall mean an electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory,

b) it is created using means that the signatory can maintain under his sole control,

c) it is linked to the document to which it relates in such a manner that any change to the data of the communication or document made subsequent to the execution of the signature is detectable.

16) 'Time-stamp' shall mean a form of verification that is permanently attached to or logically associated with an electronic communication or document, to include the time of stamping, and that is technically linked to the document to which it relates in such a manner that any change to the data subsequent to certification is detectable.

17) 'Qualified electronic signature' shall mean an advanced electronic signature created with a secure-signature-creation device and which is attested by a qualified certificate.

18) 'Qualified certification-service-provider' shall mean a certification-service-provider registered according to Subsection (3) of Section 8.

19) 'Qualified certificate' shall mean a certificate which meets the requirements laid down in Schedule No. 2 to this Act and is provided by a qualified certification-service-provider.

20) 'Service procedures' shall mean the administrative and management procedures applied by a service provider defined in Subsection (1) of Section 6.

21) 'Certificate' shall mean an attestation issued by a certification-service-provider which - according to Subsections (3) or (4) of Section 9 - links signature-verification data to a person and confirms the identity of that person.

Section 3.

(1) Acceptance of an electronic signature, or an electronic communication or document, including if used as evidence, cannot be denied and their suitability for legal statement and their legal force cannot be disputed, Subsection (2) notwithstanding, solely on the grounds that the signature, or the communication or document exists only in electronic format.

(2) In connection with the legal relationships referred to in Sections 598-684 of the Civil Code of the Republic of Hungary and in Act IV of 1952 on Marriage, Family and Legal Custody, the relevant

documents and other correspondence cannot be made with electronic signatures and in electronic format only, by abolishing the use of any format other than electronic.

(3) In the various types of court proceedings, in addition to use as evidence under Subsection (1), official actions may be implemented by electronic communications and documents, and electronic signatures only - abolishing the use of any documents other than those in electronic format - if this is expressly permitted by legal regulations which govern the type of proceeding in question.

(4) In administrative procedures by the authorities of the various sectors, in addition to use as evidence under Subsection (1), official actions may be implemented by electronic communications and documents, and electronic signatures only - abolishing the use of any documents other than those in electronic format

a) if this is expressly permitted by legal regulation which governs the type of proceeding or the relevant sector, and as pertains to the case in question,

b) in respect of local government, administrative and official matters, if the criteria under Paragraph a) exist and the local government has adopted a legal regulation to permit administration in electronic format under its jurisdiction.

(5) In the cases defined in Subsections (3) and (4), if the law prescribes written documents, it may be satisfied using electronic communications as well.

(6) The Government may implement other requirements by decree concerning electronic documents made by central administration agencies and local authorities, the electronic signatures used for such documents, and the associated certificates and the certification-service-providers attesting such certificates.

(7) Use of electronic signatures by clients cannot be rendered mandatory by law, except for the legislation which governs the method of taxation.

(8) Qualified certificates must be accepted in all the court or administrative procedures defined in Subsections (3) and (4).

Legal Recognition of Electronic Documents and Services Related to Electronic Signatures

Section 4.

(1) If written form of documentation is prescribed by statute for any legal relationships other than those defined in Subsections (2)-(4) of Section 3, electronic communications shall also be sufficient to satisfy this criteria if signed by advanced electronic signatures.

(2) If an electronic document, other than an electronic statement, is sealed with a qualified electronic signature, it is to be presumed that no change to the data of the document has been made subsequent to the execution of signature, unless otherwise indicated by the signature verification process.

(3) Any printout of an electronic document executed by an advanced or qualified electronic signature shall not be covered by the regulations governing admissibility as evidence of the same document made in electronic format.

(4) Any electronic-signature product that has been certified by an organization appointed by the Minister of Information Technology and Communications (hereinafter referred to as "Minister") or accredited by an accreditation committee according to Act XXIX of 1995 on the Accreditation of Laboratories and Certification and Authentication Organizations and is authorized to provide certification services, or by a certification body defined in Subsection (3) of Section 7, it shall be presumed - unless proven to the contrary - that such electronic-signature product is secure and that it satisfies all other criteria specified in the certificate.

(5) If signature-creation data is placed in a signature-creation device by a service provider registered as a qualified service provider for the service in question at the time when the data was placed, it shall be presumed - unless proven to the contrary - that the signature-creation data is controlled exclusively by the person to whom the service is provided.

(6) If time-stamping has been executed by a service provider registered as a qualified service provider it shall be presumed - unless proven to the contrary - that no change to the data of the document has been made subsequent to the execution of time-stamping unless otherwise indicated by the time-stamping verification process.

(7) Within the meaning of Subsections (2), (7) and (8) of Section 3, other legal ramifications may be stipulated by law in connection with services related to electronic documents and electronic signatures.

Section 5.

(1) Certificates issued by foreign-registered certification-service-providers or whose domicile is located abroad (hereinafter referred to as "foreign") shall be subject to the provisions of this Act and to the legal ramifications defined in Subsection (7) of Section 4, if

a) so stipulated by treaty, or

b) a certification-service-provider established in Hungary (hereinafter referred to as "domestic") guarantees - in the manner defined in Subsections (4)-(6) - the certificates issued by a foreign certification-service-provider, or

c)

(2)

(3) For the guarantees by domestic certification-service-providers under Paragraph b) of Subsection (1) the provisions of Subsections (4)-(6) shall apply.

(4) Domestic certification-service-providers may guarantee the certificates issued by foreign certification-service-providers by contract with their liability limited as defined in Subsection (2) of Section 9.

(5) The guarantee defined in Subsection (4) may be provided in a fashion whereby the domestic certification-service-provider issues another certificate by order of the foreign certification-service-provider (hereinafter referred to as "re-certification"), which the foreign certification-service-provider may attach to his own certificate.

(6) Certification-service-providers shall forthwith notify the Communications Agency (hereinafter referred to as "Agency") concerning any guarantee and re-certification they issue. The Agency shall publish the guarantees issued, their type and limitations and the foreign certification-service-provider involved, and shall indicate that the domestic certification-service-provider in question is classified under Subsection (1) of Section 7 or under Subsection (1) of Section 8.

(7) The certificates attested by a foreign certification-service-provider not referred to in Subsections (1) or (2) shall be subject to the legal ramifications defined in Subsection (1) of Section 3.

Services

Section 6.

(1) Services related to electronic signatures (hereinafter referred to as "services") are the following:

a) electronic signature certification service (hereinafter referred to as "certification service"),

b) time-stamping,

c) placing signature-creation data on a signature-creation device.

(2) Certification service includes the service provider establishing the identity of the person requesting the service, issuing certificates and providing other services related to electronic signatures, such as keeping records, updating any changes in the data of certificates, and publishing the procedures associated with certificates, the signature-verification-data and information pertaining to the current status of certificates (in particular if revoked).

(3) Time-stamping entails the service provider to attach a time-stamp to an electronic document. Time-stamps shall be subject to the provisions covering certificates, qualified time-stamps and qualified certificates.

(4) The services defined in Paragraphs a)-c) of Subsection (1) may be provided individually or in any combination. Qualified certification-service-providers shall be authorized to issue certifications which are not qualified, and to issue certificates under variable conditions (i.e. maximum guaranteed limit) (hereinafter referred to as "type of certificate").

(5) Time-stamping service providers and users of signature-creation data defined in Paragraph c) of Subsection (1) above and the commencement, provision and conclusion of these services shall be subject to the provisions pertaining to certification-service-providers and to the commencement, provision and conclusion of certification services.

(6) Service contracts shall be deemed valid only if made in writing.

Conditions for the Provision of Services

Section 7.

(1) Secure services may be provided by natural persons of domestic domicile or residence or by legal persons and other entities and organizations established or having business premises in Hungary subject to notification of the Agency within 30 days before commencing the activities. The service procedures and the general contract terms and conditions shall be attached with the notification.

(2) Advanced and qualified electronic signatures and time-stamping may be created only by using such signature device or other electronic-signature product that has been attested by an accredited organization registered by the Agency. The Agency shall check the existence of this criteria upon registering the signature device or the service provider, or subsequent to registration.

(3)

Section 8.

(1) When a service provider wishes to provide any of the qualified services defined in Subsection (1) of Section 6, a certificate shall be obtained from the Agency to attest that the service provider has satisfied the personnel, technical and other criteria specified in Subsections (4) and (5), which are necessary for the provision of such services.

(2) The application for qualification shall have the relevant documents attached so as to prove that the service provider and/or his employee has no prior criminal record, as well as a certificate of education, the service procedures and other documents to verify satisfaction of any additional requirements prescribed by law above and beyond those stipulated in Subsection (4). Liability insurance and access to other financial resources shall also be verified.

(3) Registered qualified service providers shall be entitled to denote their being qualified in the certificates they issue.

(4) Qualified certificates and time-stamping services may be provided by the service providers who satisfy the following requirements:

a) the natural person, or the executive employee or director of the legal person or other entity or organization has no prior criminal record;

b) the natural person, or the executive employee or director of the legal person or other entity or organization has the training or schooling prescribed in a separate legal regulation;

c) has sufficient liability insurance coverage and financial background to demonstrate the reliability necessary for providing certification services;

d) meets the criteria laid down in Schedules Nos. 1 and 3 to this Act for providing certification services.

(5) The Agency shall be entitled to check the criminal record of the applicants.

Certification Services

Section 9.

(1) Prior to contracting the service provider shall inform the client concerning the manner of using the service, the degree of security, the service procedures and the contract terms and conditions, in particular the limitations defined in Subsection (2).

(2) Certification-service-providers may stipulate the attributes, the geographical extent and other limitations for use of the certificate, and the maximum value of liability applicable to any one certificate.

(3) Under the authorizations defined in Section 12, the certification-service-provider shall establish the identity of the client and authenticate the electronic signature of the client by issuing a certificate executed by his own electronic signature.

(4) The certificate shall contain the data defined in Schedule No. 2 to this Act verified as authentic. Users of these services shall be entitled to request the certification-service-provider to indicate in the certificate a pseudonym instead of the signatory's name

(5) Certification-service-providers must ensure that the signature-creation data and/or the signature-verification-data is unique, and can be used in convergence if both originate from the certification-service-provider.

(6) Certification-service-providers shall administer any changes in the data of certificates and shall update their records so as to show the current status of certificates and shall indicate if it is suspended or revoked. These records and the service provider's service procedures, the signature-creation data and the list of revoked certificates shall be displayed to allow access to the general public through public telephone networks at all times.

(7) Certification-service-providers shall retain all electronic information associated with their certificates, including those used for issuing such certificates, and the related personal data for at least ten years from the date when the certificate to which they pertain expired, or until the definitive conclusion of any litigation in connection with the electronic signature or the electronic document executed by the electronic signature; furthermore, service providers shall provide a device within the above-specified time limit that is suitable to establish the contents of certificates they issued.

(8) Certification-service-providers shall only be allowed to suspend the issue of new certificates; all other services must be provided without any interruption.

Section 10.

(1) Certification of an electronic signature may be issued to serve as an authorization for the signatory to sign in the name and on behalf of another person (organization). In this case the provision pertaining to the user of the certification service and the signatory shall apply to the representative.

(2) A certificate defined in Subsection (1) may be issued if the power of representation is properly verified. The certification-service-provider must ensure that a power of attorney is available and shall notify the person (organization) represented when issuing the above-specified certificate.

(3) If the power of representation is terminated the certification-service-provider shall revoke the certificate indicating the power of representation if requested by the person (organization) by whom or to whom such power was delegated.

(4) The certificate defined in Subsection (1) may indicate a pseudonym only if approved by the person represented.

Data Processing and Data Protection

Section 11.

(1) Certification-service-providers may collect personal data only directly from the signatory, or after the explicit consent of the signatory, and only insofar as it is necessary for the purposes of issuing the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject, and - with the exceptions set forth in Subsections (2) and (3) - may not be conveyed to third parties.

(2) For the purposes of prevention and detection of criminal offences involving electronic signatures and for national security reasons, certification-service-providers shall provide information to the acting investigation authority or the national security service to establish the identity of the person implicated and concerning the data referred to in Subsection (2) of Section 12 if the criteria prescribed by law for requesting data are satisfied. Any data and information supplied shall be recorded. The certification-service-provider shall not notify the data subject concerning the disclosure of such data.

(3) In connection with civil lawsuits and nonlitigious proceedings which concern the validity of a certificate, the certification-service-providers shall provide information to the opposing party or his proxy - if their interest is properly verified - to establish the identity of the signatory and concerning the data referred to in Subsection (2) of Section 12, or shall disclose such data to the court upon request.

(4) If a pseudonym is indicated instead of the signatory's name, with the exceptions set forth in Subsections (2) and (3), the certification-service-provider shall disclose any data concerning the true identity of the signatory only upon the explicit consent of the signatory or the person (organization) represented according to Subsection (4) of Section 10, to the authorities or any third party.

Section 12.

(1) Certification-service-providers shall be entitled to check the identification document, passport, driver's license or other identification paper of the signatory in order to establish his/her identity.

(2) Certification-service-providers shall consult the following agencies for reference, with their name and the purpose of data processing indicated;

a) for checking the identity of a signatory either of the agencies for personal data and address records, passports records, or driver's license records,

b) for checking power of representation, the company register.

Signatory

Section 13.

(1) The signatory shall be entitled to control his signature-creation data and shall forthwith disclose the following to the certification-service-provider:

a) personal identification data suitable to establish his identity, regarding his power of representation to sign in the name and on behalf of another person (organization) by electronic signature, the personal identification data of the person on whom such power is conferred, the data defined in Paragraphs d) and k) of Schedule No. 2 to this Act, furthermore, corporate data and any changes in the above;

b) notification if his signature-creation data was lost or was conveyed to any unauthorized person;

c) any discrepancies concerning the signature or any electronic document executed by his signature, that are defined by legal regulation or by the service procedures;

d) if any lawsuit is filed in connection with an electronic document for which a certificate was issued.

(2) The signatory shall be liable for any and all damages resulting from his failure to comply with the obligations defined in Subsection (1).

(3) The signatory or the person (organization) represented under Section 10 may request the certificate to be suspended or revoked.

(4) The signatory may use the signature-creation data solely for the creation of an electronic signature in due observation of any other limitations indicated in the certificate.

Suspension or Revocation of a Certificate by the Service Provider of Issue

Section 14.

(1) The certification-service-provider shall suspend the certificate he has issued and shall publish such action forthwith if

a) it is requested by the signatory or the person (organization) represented;

b) any discrepancy from the provisions of legal regulations related to the service, the service procedures or the general contract terms and conditions is detected;

c) it is alleged that any data of the certificate is false or if the signature-creation data is not controlled exclusively by the signatory;

d) so prescribed by a definitive and executable resolution of the Agency.

(2) The certification-service-provider shall revoke the certificate he has issued and shall publish such action forthwith if

a) it is requested by the signatory or the person (organization) represented;

b) the discrepancy defined in Paragraph b) of Subsection (1) cannot be remedied;

c) it is alleged that any data of the certificate is false or if the signature-creation data is not controlled exclusively by the signatory;

d) so prescribed by a definitive and executable resolution of the Agency;

e) his certification service is terminated;

f) the certificate has expired.

(3) No certificate shall be revoked retroactively.

(4) The general contract terms and conditions and/or the service procedures shall contain a clause to indicate the legal consequences if the certificate is revoked before it expires.

Liability of Service Providers

Section 15.

(1) Certification-service-providers shall be subject to liability according to Section 339 of Act IV of 1959 on the Civil Code of the Republic of Hungary with respect to third parties who are not under any contractual relationship with the service provider, and according to the provisions governing breach of contract with respect to the signatory for damages arising in connection with qualified electronic signatures and time-stamps or electronic documents executed by such, if he has violated the provisions of Subsection (2) of Section 7, Sections 9-11 and/or Section 14. In case of any doubt, burden of proof lies with the service provider regarding compliance with these provisions.

(2) Certification-service-providers shall not be held liable for claims or damages arising in connection with electronic documents issued and executed in excess of the limitations specified in Subsection (2) of Section 9.

(3) Any person (organization) under guarantee obligation according to Subsection (2) of Section 5 shall be subject to joint and several liability with the foreign certification-service-provider according to Subsection (1) for damages caused to a domestic user in connection with a qualified electronic signature.

Termination of Certification-service-provider's Activities

Section 16.

(1) The certification-service-provider who wishes to terminate his activities shall notify the persons indicated as signatories in the certificates he has issued and which are still valid, and the Agency at least sixty days before the planned date of termination, and indicate the organization defined in Subsection (2). As of the date of the notification the certification-service-provider may not issue new certificates. The certification-service-provider must revoke all certificates he has issued and which are still in circulation at least twenty days before the planned date of termination. After the certificates are revoked the certification-service-provider remains under the obligation of publication [Subsection (2) of Section 6] until his activities are terminated.

(2) The certification-service-provider about to terminate his activities must ensure that the records defined in Subsection (6) of Section 9 are taken over by another certification-service-provider of the same classification on or before the date of termination, in particular the directory of revoked certificates, and that the replacement service provider satisfies the obligations defined in Subsection (7) of Section 9. All data related to revoked certificates, including personal data, must be handed over.

(3) The Agency shall appoint an organization under Subsection (2) if one is not indicated by the certification-service-provider in the notification defined in Subsection (1).

(4) If a certification-service-provider fails to notify termination of his activities in advance and fails to satisfy the obligation defined in Subsection (2), the Agency shall take immediate action to have the certificates issued by such service provider revoked and shall publish this action, and shall appoint a certification-service-provider to carry out the obligation defined in Subsection (7) of Section 9 and to retain the data defined in Subsection (6) of Section 9. All related costs of the Agency shall be borne by the certification-service-provider terminating his activities.

(5) The certification-service-provider who is adjudicated in bankruptcy or is under liquidation shall notify the Agency forthwith to that effect, and shall indicate the name of the proceeding organization. The Agency shall be entitled to inquire at this organization concerning the status of the proceedings, and if the certification-service-provider fails to submit the notification defined in Subsection (1) by the date when the closing statement of affairs is submitted, the Agency shall appoint the organization defined in Subsection (2).

(6) The Agency shall remove the certification-service-provider from the register if dissolved or if service activities are terminated.

Responsibilities of the Agency

Section 17.

(1) The Agency

a) shall register the service providers defined in Subsection (1) of Section 7 and in Subsection (1) of Section 8, and the persons (organizations) defined in Subsection (2) of Section 7;

b) shall monitor and investigate - prior to the qualification procedure, during and after notification and during operations - the service provider's compliance with the provisions of this Act and other legal regulations implemented under authorization by this Act, and the provisions of the service procedures and the general contract terms and conditions;

c) shall take the measures and implement the sanctions defined in Sections 21-23 in the event of non-compliance with the requirements laid down in Paragraph b);

d) shall keep various records and directories and shall display these records and directories to allow access to the general public through public telephone networks at all times.

(2) The proceedings of the Agency shall be governed by Act IV of 1957 on the General Rules of State Administration Procedures with the deviations stipulated in this Act.

(3) Any resolution of the Agency concerning measures and penalties shall be executable forthwith.

(4) The Agency shall resolve all applications and petitions within sixty days from the date of receipt.

(5) The Agency's resolutions cannot be altered or annulled under supervisory functions, and cannot be appealed against under administrative procedures. These resolutions may be contested in court within thirty days from the date when served.

(6) The Agency may be assisted by judicial experts or other persons having proper expertise.

(7) The Agency's services in connection with qualifications and registrations shall be subject to a fee, which is payable to the Agency. The penalties levied under this Act shall be payable to the central budget.

Qualification Procedure

Section 18.

(1) In the qualification procedure the Agency shall investigate the service provider's compliance with

a) technical and other operating requirements, in particular the criminal record and education of employees and whether they are sustained on a continuous basis;

b) legal regulations, the service procedure and the general contract terms and conditions.

(2) If the qualification procedure confirms that the applicant service provider satisfies the requirements laid down in this Act and in legal regulations implemented under authorization by this Act, the Agency shall register the applicant as a certification-service-provider authorized to issue qualified certificates.

(3) The service provider who fails to satisfy the requirements set forth in Subsection (1) shall not be registered.

(4) If any change occurs in the service provider's particulars, the Agency must be notified without delay and the qualification procedure shall be repeated. During the repeated procedure the Agency

shall not investigate compliance with the criteria that were checked previously, provided that these criteria are not affected by the change.

Records and Directories

Section 19.

The Agency shall keep, and display, the following records and directories:

a) Register of service providers qualified according to Subsection (1) of Section 8 and registered according to Subsection (1) of Section 7, indicating the name, address (residence, business, office) of the service provider, the type of services authorized, the serial numbers of signature-creation-devices provided and the other electronic-signature products offered by the service provider, along with other data stipulated by law.

b) Register of signature-creation-devices defined in Subsection (2) of Section 7 and other electronic-signature products, for which a code is assigned when registered.

c) Register of organizations accredited for the certification of signature-creation-devices used for advanced and qualified electronic signatures and other electronic-signature products, including the name of the organization, the manner of contact, its field of specialty, and other data stipulated by legal regulation.

d) Register of certificate types to be issued by a qualified certification-service-provider, for which a code is assigned when registered.

Supervision of Service Providers, Measures

Section 20.

(1) The Agency shall have powers to oversee whether the service provider complies with the provisions of this Act and other legal regulations implemented under authorization by this Act, the service procedures and the general contract terms and conditions, and carries out the Agency's resolutions and measures.

(2) The Agency shall be entitled to conduct on-site inspections upon providing proof of authorization. The Agency's inspector shall have powers to enter the premises of operations of the service provider, to inspect documents, data mediums, articles and work processes, to interrogate or to request information from the representative or employee of the certification-service-provider. The service provider inspected shall cooperate to render the inspection possible.

(3) The Agency shall conduct comprehensive inspections at least once a year at qualified certification-service-providers.

Section 21.

(1) In order to enforce the provisions of this Act and other legal regulation implemented under authorization by this Act, the service procedures and the Agency's resolutions, and to prevent or terminate unlawful acts and discrepancies, the Agency shall have powers to take the following measures:

a) notify the service provider to comply with the requirements laid down in the provisions and resolutions defined in Subsection (1);

b) ban the use of certain technologies or procedures;

c) temporarily suspend the service provider's license to issue new certificates, and shall indicate this in the register;

d) order the revocation of qualified certificates previously issued;

e) levy a fine;

f) remove the service provider from the register of qualified certification-service-providers.

(2) The Agency shall implement the measures defined in Subsection (1) upon weighing the gravity and frequency of the unlawful act, the extent of potential or actual damage, the classification of the service provider and whether the certification-service-provider was subject to any disciplinary action in the past. Measures may be implemented individually or combined.

(3) The Agency shall remove the service provider from the register whose registration should have been denied, or if the conditions stipulated in this Act and in other legal regulations implemented under authorization by this Act cannot be ensured otherwise. A service provider can be removed from the register only if other measures proved ineffective.

(4) When a qualified certification-service-provider is removed from the register the Agency shall ban the service provider from using the denotation "qualified" on the certificates he has issued.

(5) When a qualified certification-service-provider is removed from the register the Agency shall concurrently implement the provisions laid down in Subsection (4) of Section 16.

(6) By order of the Agency a qualified certificate that is alleged to contain false or forged data shall be revoked, also if the signature-creation device the qualified certification-service-provider used for the signature of qualified certificates is not secure.

Penalties

Section 22.

(1) Any certification-service-provider who fails to satisfy the obligations stipulated in this Act and in other legal regulations implemented under authorization by this Act, the service procedures and the Agency's resolutions shall be subject to penalty. With regard to repeat offences, or if the certification-service-provider fails to carry out the Agency's resolution or to perform the obligation defined in Subsection (2) of Section 20, the executive employee of the certification-service-provider may also be penalized simultaneously with the service provider.

(2) No penalty may be levied after two years from the date when the Agency gains knowledge of the offence or breach of obligation, or after maximum three years from the date when committed.

(3) The Agency shall determine the amount of penalty

a) as consistent with the extent of risk or damage resulting from the offence or negligence,

b) with due consideration to the degree of cooperation provided by the responsible persons with the Agency (in particular producing documents and records for inspection, demonstration of applied technologies and specifications),

c) in view of whether the person implicated acted in good or bad faith,

d) in view of whether any relevant data, material or information is concealed, or attempts were made to conceal such,

e) the history of repeat offences.

Section 23.

(1) The amount of penalty shall be between 100,000 and 10,000,000 HUF if

a) a certification-service-provider who is not registered as a qualified certification-service-provider issues a qualified certificate, or denotes himself as a qualified certification-service-provider in a certificate he has issued, or implies it directly or indirectly;

b) a certification-service-provider fails to take the necessary measures to ensure adequate protection of his own signature-creation data;

c) fails to retain the data and documents used for the issue of a certificate until the time limit prescribed by legal regulation or by the service procedures, and no protection is provided any other way.

(2) For offences not described in Subsection (1) the penalty shall be between 50,000 and 5,000,000 HUF.

(3) The amount of penalty levied on executive employees shall be between 50,000 and 1,000,000 HUF.

Certification Bodies

Section 24.

(1) Certification bodies for the attestation of signature devices and other electronic-signature products shall be appointed by the Minister. Applications for licensure as certification bodies may be submitted by natural persons and organizations who have the expertise necessary for the attestation of signature devices and other electronic-signature products.

(2) The appointed certification bodies and those accredited by an accreditation committee according to Act XXIX of 1995 on the Accreditation of Laboratories and Certification and Authentication Organizations to perform the services defined in Subsection (1) shall be registered by the Agency.

(3) Certification bodies shall be unbiased during the attestation procedure of signature devices and other electronic-signature products.

(4) Appointment and accreditation shall be revoked and the certification body shall be removed from the register if it does not have the necessary requirements, or if the certification body fails to operate in compliance with legal regulations. If the Agency detects any of the above in connection with a body referred to in Subsection (2), it shall notify the Minister or the accreditation committee, as appropriate.

(5) Whenever a certification body is removed from the register it shall not affect the validity of the certificates issued previously.

Closing Provisions

Section 25.

Within the framework of Section 3 of Act I of 1994 promulgating the Europe Agreement establishing an association between the Republic of Hungary and the European Communities and their Member States, signed in Brussels on 16 December 1991, this Act contains regulations designed to approximate the following legal regulations of the European Communities:

a) Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures, and

b) Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) Article 9 (2).

Section 26.

(1) This Act, with the exceptions set forth in Subsections (2) and (3), shall enter into force on the first day of the third month following its promulgation. The provisions contained therein shall be applied to the electronic documents produced subsequently and the electronic signatures by which

these document are executed. Subsection (1) of Section 3 and Subsection (7) of Section 5 shall also apply to the electronic documents and the electronic signatures produced previously.

(2) The reference in Subsection (4) of Section 4 to Subsection (3) of Section 7; Paragraph c) of Subsection (1) of Section 5 and Subsection (2) of Section 5; the reference in Subsection (7) of Section 5 to Subsection (2) of Section 5; and Subsection (3) of Section 7 shall enter into force simultaneously with the Act promulgating the treaty on the accession of the Republic of Hungary to the European Union.

(3) Paragraph b) of Subsection (2) of Section 27 shall enter into force on the eighth day following the date of promulgation.

Section 27.

(1) The Government is hereby authorized to decree

a) the powers and responsibilities of the Agency in connection with this Act, the detailed regulations of the proceedings under this Act and the related records to be maintained, their contents, the type of data other than personal to be obtained for the proceedings and the organization from which to obtain them;

b) the requirements specific to the electronic documents made by central administrative agencies and local authorities, and the electronic signatures used for such documents and the associated certificates and the certification bodies.

(2) The Minister is hereby authorized to decree

a) the detailed criteria pertaining to services related to electronic signatures and the providers of such services;

b) the regulations concerning the certification bodies accredited for the attestation of signature-creation devices used for advanced and qualified electronic signatures and of other electronic-signature products, and the regulations for the accreditation of such bodies;

c) the rates of fees to be charged by the Agency under this Act for its services in agreement with the Minister of Finance.

(3) The ministers are hereby authorized to decree, in agreement with the Minister of Information Technology and Communications, concerning the sectors they govern

a) the types of legal relationships, in which electronic communications and documents shall be accepted as the only way of documentation of the relevant administrative proceedings;

b) the regulations specific to the administration procedures in which electronic communications, electronic documents and electronic signatures are used.

(4) The Minister directing the Prime Minister's Office is hereby authorized to decree the criteria and requirements for implementing and operating the Government's electronic signature system.

(5) The local governments are hereby authorized to determine the types of services provided to the general public and the types of administrative proceedings for which electronic communications and documents may be used exclusively within their respective jurisdictions and as consistent with the higher level statutes governing the proceeding in question.

Section 28.

(1) The following provision shall replace Subsection (2) of Section 38 of Law-Decree No. 11 of 1960 on the Entry into Force and Implementation of Act IV of 1959 on the Civil Code of the Republic of Hungary (hereinafter referred to as "EICLD"):

(2) If legal regulation stipulates the validity of a contract subject to be made in writing, it shall be deemed satisfied - unless otherwise prescribed by legal regulation - if the agreement is made by way of correspondence through the mail, telegraphic messages or telex, or through any other permanent

means defined in a separate statute, in particular by way of document executed by electronic signature."

(2) The following Subsection (3) shall be appended to Section 38 of EICLD, and simultaneously the current numbering of Subsection (3) shall be changed to Subsection (4):

(3) If the parties stipulate the validity of their contract subject to be made in writing, this clause may also stipulate the type of written form defined in Subsection (2) to satisfy this criteria."

Section 29.

(1) The following provision shall amend Paragraph e) of Subsection (1) of Section 196 of Act III of 1952 on the Code of Civil Procedures (hereinafter referred to as "CPC"), and simultaneously the following new Paragraph f) shall be appended:

(Private documents shall be admissible as evidence, unless proven to the contrary, that the issuer has made, approved or recognized as mandatory the statement which it contains, provided that any of the criteria below prevails:)

e) a document made and duly signed by an attorney (legal counsel) is provided, in which the attorney (legal counsel) declares that the issuer has signed the document in front of him or has declared the signature as his own, or the electronic document executed by the qualified electronic signature of the issuer contains the same data as the electronic document made by the attorney;

f) the electronic signature of the issuer on the electronic document is qualified."

(2) The following provision shall replace Subsection (2) of Section 197 of CPC:

(2) If the authenticity of the signature on a private document is not disputed or it is proven, and unless otherwise indicated by the verification process of an advanced electronic signature, the text preceding the signature - or the data signed in respect of electronic statements - shall be presumed not forged unless proven to the contrary, except if the discrepancies or defects in the statement contradict this presumption."

(3) The following new Subsection (4) shall be appended to Section 197 of CPC, and simultaneously the current numbering of Subsection (4) shall be changed to Subsection (5):

(4) If the identity of the signatory of an electronic document executed by an advanced electronic signature or the authenticity of the document is doubtful, to resolve such doubt the court shall first and foremost contact the certification-service-provider who has issued the certificate to attest the advanced electronic signature in question. In case there is any doubt concerning the data verified by a time-stamp associated with an electronic document, the court shall first and foremost contact the provider of the time-stamping service."

Section 30.

The following provision shall replace Subsection (2) of Section 82 of Act I of 1973 on Criminal Procedures:

(2) For the purposes of this Act, admissible evidence shall mean documents, drawings and all objects designed to record data by technical, chemical or some other technique. Wherever this Act refers to documents, it shall also be understood as the data recording device."

Section 31.

(1) The following provision shall replace Subsection (6) of Section 3 of Act IV of 1957 on the General Rules of State Administration Procedures (hereinafter referred to as "SAPR"):

(6) This Act shall be applied concerning the matters under the following sectors and those governed by the following acts, and unless otherwise prescribed by legal regulation:

a) defense,

b) foreign trade administration,

c) social insurance, family welfare support,
d) tax, excise and customs administration,
e) industrial property rights,
f) alien control and immigration,
g) certain activities concerning atomic energy,
h) Act on Prohibition of Unfair Market Practices and Restraint of Trade,
i) the Price Regulation Act,
j) Act on Insurance Institutions and the Insurance Business,
k) Act on Credit Institutions and Financial Enterprises,
l) Act on Securities Trading, Investment Services and the Stock Exchange,
m) Act on Voluntary Mutual Insurance Funds,
n) Act on Private Pension and Private Pension Funds,
o) the Real Estate Registration Act,
p) the Electronic Signatures Act."

(2) The following provision shall replace Subsection (1) of Section 16 of SAPR:

(1) Petitions concerning state administration matters shall be submitted verbally or in writing to a public administration agency. Law may stipulate that these petitions shall be submitted on specific forms, and law may allow these petitions to be submitted in electronic documents in a specific electronic format."

(3) The following provision shall replace Subsection (3) of Section 28 of SAPR:

(3) The provisions pertaining to official documents shall apply to all objects which are, in general, designed to record data using some technical or chemical technique (photograph, video or sound recording, magnetic disc or tape, electronic document etc.)."

(4) The following provision shall replace Subsection (5) of Section 43 of SAPR:

(5) Law may require administrative agencies to issue their resolutions, including those defined in Sections 50-53, on the prescribed official forms, and may allow the communication of these resolutions in electronic documents."

(5) The following provision shall replace Subsection (1) of Section 45 of SAPR:

(1) Resolutions shall be delivered by service of process, or if the client is present they may be announced unless this is precluded by legal regulation. Legal regulation may allow the communication of the resolutions, including those defined in Sections 50-53, in electronic documents."

Section 32.

(1) The following provision shall replace Subsection (5) of Section 22 of Act CXLV of 1997 on the Register of Companies, Public Company Information and Court Registration Proceedings (hereinafter referred to as "CRA"):

(5) Applications for registration and their appendices may be submitted in the form of electronic documents through a computer network. In this case the court of registry shall file the document in electronic format."

(2) The following provision shall replace the second sentence of Section 59 of CRA:

Subsection (5) of Section 22 shall enter into force simultaneously with the legal provisions on the use of electronic documents in company registration procedures."

Section 33.

The following provision shall replace Paragraph b) of Subsection (1) of Section 27 of Act XI of 1998 on Attorneys:

(By countersigning a document the attorney verifies that)

b) the party indicated in the document has signed the document in front of him or his proxy [Subsection (5) of Section 23] or has declared the signature as his own in front of him or his proxy, or - when countersigning by his qualified electronic signature - that the electronic document executed by the qualified electronic signature of the issuer contains the same data as the electronic document made by the attorney."

Schedule No. 1 to Act XXXV of 2001

Requirements for secure signature-creation devices

1) Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:

a) the signature-creation-data used for signature generation can practically occur only once for any one signatory, and that their secrecy is reasonably assured,

b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and can be reliably protected by the legitimate signatory against the use of others, and that the signature is protected against forgery using currently available technology.

2) Secure signature-creation and signature verification devices must not alter the electronic document to be signed or prevent such data from being presented to the signatory prior to the signature process.

Schedule No. 2 to Act XXXV of 2001

Certificates must contain:

a) an indication that the certificate is issued as a qualified certificate or an advanced signature certificate,

b) the identification of the certification-service-provider and the address (State) where established,

c) the name of the signatory or a pseudonym, which shall be identified as such,

d) provision for a specific attribute of the signatory as specified by law, the service procedures or the general contract terms and conditions, depending on the purpose for which the certificate is intended,

e) signature-verification data which corresponds to signature-creation data under the control of the signatory,

f) an indication of the beginning and end of the period of validity of the certificate, and the period of time covered by the certification-service-provider in respect of the requirement specified in Subsection (7) of Section 9.

g) the identity code of the certificate,

h) the advanced electronic signature of the certification-service-provider issuing it,

i) limitations on the scope of use of the certificate, if applicable,

j) limits on the applicability of the certificate,

k) an indication if the certificate provides power of representation to another person (organization) and the particulars of this person (organization).

Schedule No. 3 to Act XXXV of 2001

Requirements for certification-service-providers issuing qualified certificates

Qualified certification-service-providers must

a) demonstrate the reliability necessary for providing certification services;

b) ensure the operation of a prompt and secure certificate and data storage facility and a secure and immediate suspension and revocation service;

c) ensure that the date and time when a certificate is issued, suspended or revoked can be determined precisely;

d) verify, by appropriate means, the identity and, if applicable, any specific attributes of the person to whom a qualified certificate is issued;

e) satisfy the requirements laid down by legal regulation concerning employees, executive officers, and organizational and operational structure;

f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

h) maintain sufficient financial resources stipulated in a separate legal regulation to operate in conformity with the requirements laid down in this Act, in particular to bear the risk of liability for damages by obtaining appropriate insurance;

i) record all relevant information concerning a qualified certificate at least for the period of time defined in Subsection (7) of Section 9, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

j) not store or copy signature-creation data of the person to whom the certification-service-provider provided services to install signature-creation data on a signature-creation device;

k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature, inform that person by durable means of communication of the existence of a voluntary accreditation scheme and that the certificate is qualified including the implications of this qualification, the precise terms and conditions regarding the use of the certificate, including any limitations on its use, and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be written in Hungarian and in readily understandable language, a copy of which shall be provided to the signatory when contracting. Relevant parts of this information, specified in a separate legal regulation, must also be made available on request to third-parties who are under or who plan to establish some relationship with the signatory;

l) use trustworthy systems to store certificates in a verifiable form to ensure that

- only persons authorized by the certification-service-provider can make entries and changes,
- information can be checked for authenticity,
- data used for issuing certificates are publicly available for retrieval in only those cases for which the signatory's consent has been obtained,
- any technical changes compromising these security requirements are apparent to the competent employees of the certification-service-provider.

Schedule No. 4 to Act XXXV of 2001

Recommendations for secure signature verification

During the signature-verification process it should be ensured with reasonable certainty that:

a) the data used for verifying the signature correspond to the data displayed to the verifier,

b) the signature is reliably verified and the result of that verification is correctly displayed,

c) the verifier can, as necessary, reliably establish the contents of the signed electronic communication,

d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified,

e) the result of verification and the signatory's identity are correctly displayed,

f) the use of a pseudonym is clearly indicated,

g) any security-relevant changes can be detected.