

# 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 executed with electronic signatures 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 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 who holds a signature-creation device and acts either on his own behalf or on behalf of another person.
- 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 in electronic form which are attached to or logically associated with other electronic data or 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, the certificate and any information concerning the revocation of 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, software or relevant components thereof that are intended

to be used for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures or time-stamps.

12) 'Electronic document' shall mean data processed by electronic means.

13) 'Electronic signature validation' shall mean the attestation - by affixing a qualified electronic signature or a time stamp that has been issued by a service provider who is considered qualified with respect to this service - that the electronic signature or time stamp affixed to the electronic document or the certificate pertaining to them was legally valid at the time the time stamp was affixed.

14) 'Validity chain' shall mean an electronic document or its image file and the series of related information (such as, in particular, certificates, information linked to certificates, signature-verification-data, information pertaining to the current status [revocation] of certificates, and the electronic signature verification data of the certification-service-provider and information concerning the revocation of the certificate) that establishes that the advanced electronic signature or qualified electronic signature and the time stamp affixed to an electronic document as well as the certificate pertaining to them were legally valid at the time the signature was executed and the time stamp was affixed.

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

*a)* it is capable of identifying the signatory;

*b)* it is uniquely linked to the signatory;

*c)* it is created using means that the signatory can maintain under his sole control; and

*d)* it is linked to the document to which it relates in such a manner that any change to the data of the 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 document intended to verify that the electronic document existed in an unaltered form at the time of time stamping.

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

18) 'Qualified certification-service-provider' shall mean a certification-service-provider registered according to this Act and authorized to issue qualified certificates to the public.

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 that - according to Subsection (3) or (4) of Section 9 - links signature-verification data to a person and confirms the identity of that person or some other connected deed, including whether it pertains to an authority or an official act.

22) 'Archiving-service-provider' shall mean a person providing electronic archiving services in connection with documents executed with electronic signatures in accordance with this Act.

23) 'Authentication system' shall mean a collection of instructions drawn up by the service provider, the recipient, or any other person or organization concerning the use of a certificate with regard to a group of recipients to whom the same set of security requirements apply or with regard to specific applications.

24) 'Time-stamping system' shall mean a collection of instructions drawn up by the service provider or the recipient, or any other person or organization concerning the use of a time-stamp with regard to a group of recipients to whom the same set of security requirements apply or with regard to specific applications.

25) 'Recipient of the service' shall mean a natural or legal person or unincorporated organization to which electronic-signature services are provided.

26) 'Image file' shall mean a string of bits of specific length linked to an electronic document created by a procedure (imaging procedure) that is able to satisfy the following requirements at the time when created:

*a)* the image file is clearly linked to the electronic document from which it is created;

*b)* the image file contains sufficient safeguards to prevent with reasonable security any invasion to obtain in any way or form the contents of the electronic document from which it is created;

*c)* the image file contains sufficient safeguards to prevent with reasonable security any duplication of the electronic document that can be used for the imaging procedure to create the image file in question.

27) 'Qualified service provider' shall mean qualified certification-service-providers and persons providing the services referred to in Paragraphs *b)*-*d)* of Subsection (1) of Section 6 of this Act qualified for specific services as indicated in the register of service providers.

28) 'Service provider' shall mean any natural or legal person or unincorporated organization engaged in providing electronic-signature services.

### *Section 3.*

(1) Acceptance of an electronic signature, 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 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 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 documents executed with electronic signatures, 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)

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

(6) With a view to the implementation of the provisions contained in Act CXL of 2004 on the General Rules of Administrative Proceedings and Services, the Government may prescribe special requirements by decree concerning electronic signatures that may be used in administrative proceedings and services, the certificates of electronic signatures and the related services provided in connection with electronic signatures.

(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 documents executed with electronic signatures shall also be sufficient to satisfy this criteria if signed by advanced electronic signatures.

(2) If an electronic document 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 that is 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 that is registered as a qualified service provider it shall be presumed - unless proven to the contrary - that the data of the document remained unaltered subsequent to the execution of time-stamping, unless otherwise indicated by the time-stamping verification process.

(7) If the archiving of electronic documents executed by an electronic signature is carried out by a service provider that is registered as a qualified service provider for the service in question, it shall be presumed - unless proven to the contrary - that the electronic signature or the time-stamp affixed to the electronic document and the certificate pertaining to them were legally valid at the time the signature was executed and the time-stamp was affixed.

(8) Where a copy is made of a printout of a document in electronic format as governed in specific other legislation, the electronic document containing the copy shall be subject to the same legal ramifications as those pertaining to the

original printed document.

(9) 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 executed with electronic signatures 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) the registered or home address of the certification-service-provider is in a Member State of the European Union.

(2) The certificates issued by foreign certification-service-providers shall be subject to the provisions of this Act and to the legal ramifications defined in Subsection (7) of Section 4, also if

- a) the certificates issued by the foreign certification-service-provider are guaranteed by a certification-service-provider who is established or domiciled in a Member State of the European Economic Area, or
- b) the foreign certification-service-provider satisfies the requirements laid down in the relevant directive of the European Communities, and has been accredited under the voluntary accreditation scheme established in a Member State.

(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 National Communications Authority (hereinafter referred to as "Communications Authority") 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") shall comprise 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,
- d) electronic archiving.

(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.

(4) As part of the electronic archiving services, the service provider shall

a) archive the validity chain existing at the time of archiving to ensure that the documents are properly stored and that they cannot be disclaimed;

b) ensure that the validity chain is not compromised so that the validity of electronic signatures it represents can be controlled in the long term;

c) deliver the validity chain to the recipient forthwith when so requested;

*d)* supply a certificate upon request concerning archived electronic documents executed with electronic signatures or validity chains.

(5) The services defined in Paragraphs *a)-d)* of Subsection (1) may be provided individually or in any combination. Qualified certification-service-providers shall be authorized to issue certificates that are not qualified. Certification-service-providers shall be authorized to issue certificates under variable conditions (i.e., maximum guaranteed limit, compliance with any authentication system).

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

## ***Notification***

### *Section 7.*

(1) The services referred to in Paragraphs *a)-d)* of Subsection (1) of Section 6 in connection with electronic signatures may be provided by natural persons whose permanent or habitual residence is located in Hungary or by legal persons and unincorporated organizations that are established or have business establishments in Hungary subject to notification of the Communications Authority within 30 days before commencing activities.

(2) The following shall be attached with the notification:

*a)* service procedures,

*b)* general contract terms and conditions,

*c)* a certified copy of the document that proves the applicant and his employees have no prior criminal record as well as a copy of documents proving their qualifications,

*d)* proof of liability insurance coverage and access to other financial resources as specified in specific other legislation, and

*e)* the authentication system and time-stamping system drafted, respectively, by the certification-service-provider and time-stamping service provider.

(3) Service providers shall provide a statement in which they declare whether they wish to operate as qualified service providers.

(4) The designation 'qualified' may only be used in relation to services related to electronic signatures by the qualified service providers registered according to this Act in their advertisements, on their stationary, in the certificates they have issued, or in any other way.

(5) Certificates and time-stamping, and qualified electronic signatures may be created only by using a signature device or other electronic-signature product that has been attested by an accredited organization registered by the Communications Authority. The Communications Authority shall check the existence of these criteria upon registering the signature device or the service provider, and also subsequent to registration.

(6) For the purposes of Subsection (5), any certificate issued by a certification body established in a Member State of the European Union shall be recognized.

(7) Service providers shall notify the Communications Authority of any changes in their particulars on record thirty days in advance.

### *Section 8.*

(1) Qualified service providers must at all times satisfy the following requirements:

*a)* the natural person or, if a legal person or unincorporated organization, the executive officer or director and the employees have no prior criminal record;

*b)* the natural person or, if a legal person or unincorporated organization, the executive officer or director or an employee has the training or schooling prescribed in specific other legislation;

*c)* the service provider has sufficient liability insurance coverage and financial wherewithal to demonstrate the reliability necessary for providing the services as specified in specific other legislation;

*d)* the service provider meets the criteria laid down in Schedules Nos. 1 and 3 of this Act for providing the services.

(2) The Communications Authority shall be entitled to check the criminal records of the applicants.

## ***Disclosure Requirement of Service Providers***

### *Section 8/A.*

(1) The Communications Authority shall have powers to instruct the service providers engaged in activities governed under this Act to supply data and information within the time limit specified for studies, analyses, and evaluations to the extent necessary to discharge its duties. Service providers shall supply all data requested by the deadline and in the form the Communications Authority has specified. If a service provider fails to comply with data disclosure requirements, the Communications Authority shall be authorized to apply the sanctions defined in Section 22. The Communications Authority may also request service providers engaged in activities governed under this Act to supply data, other than personal data, voluntarily within the framework of the relevant statutory provisions.

(2) The Communications Authority shall inform service providers concerning the processing and use of the data it has requested, indicating the legal objective of data processing in the notice conveyed to request specified data and information, whether compulsory or voluntary. If data is requested under Subsection (1) to be supplied compulsorily, the Communications Authority shall advise the service provider concerning the legal consequences of any infringement of the time limit or formal requirements or if the data supplied is incomplete or false and of the remedy under Subsection (4); the notice shall also contain an indication that the disclosure of data and information is not mandatory.

(3) The Communications Authority may use the data supplied by service providers engaged in activities governed under this Act within the framework of the National Statistical Data Collection Program for market research, analyses and evaluations.

(4) The Communications Authority may not use the data supplied in accordance with this Section in any proceeding conducted against the service provider. The Communications Authority shall advise the service providers of this in the notice requesting data, whether compulsory or voluntary.

## ***Voluntary Accreditation***

### *Section 8/B.*

(1) Service providers may devise voluntary accreditation schemes to enhance the level of their services, and to attest their organizational structure and the products and networks they use in the provision of services, information technology security requirements laid down in specific other legislation, or any other criteria they chose to adhere to voluntarily, and to refer to this accreditation in their advertisements, on their stationery, and in any other way.

(2) The Communications Authority shall be notified of any new voluntary accreditation scheme before it is put into operation. The notification shall include the name of the voluntary accreditation scheme as well as the name and address (residence, business establishment, place of operation) of the person or entity in charge of operating it. Any changes in the data on record shall be notified to the Communications Authority within thirty days.

(3) Service providers shall notify the Communications Authority if their organizational structure and the products and networks they use in the provision of services, information technology security requirements laid down in specific other legislation, or any other criteria they chose to adhere to voluntarily have been attested under a voluntary accreditation scheme. The notification shall include the name and address (residence, business establishment, place of operation) of the service provider, the name of the voluntary accreditation scheme, and the validity period of the attestation. Any changes in the data on record shall be reported to the Communications Authority within thirty days.

## ***Certification Services***

### *Section 9.*

(1) Prior to contracting, the service provider shall inform the recipient of the service concerning the manner of using the service, the degree of security, and - where applicable - any attestation of their organizational structure and the products and networks they use in the provision of services, information technology security requirements laid down in specific other legislation, or any other criteria they chose to adhere to voluntarily that have been attested under a voluntary accreditation scheme, and the service procedures and the contract terms and conditions, in particular the limitations defined in Subsection (2). If the inspection referred to in Subsection (3) of Section 20 is not completed at the time of commencement of the provision of services, the service provider shall inform the recipient of the service accordingly.

(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) All data contained in the certificate must be 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. Certification-service-providers shall be allowed to comply with the above obligation by way of a qualified archiving-service-provider.

(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 by Certification-Service-Providers***

#### *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) Where requested by the competent administrative agency certification-service-providers shall consult the data of a person using an electronic signature in any proceedings with that administrative agency for the purpose of

checking the identification data of this person, and shall inform the requesting authority of the results, including if there are any discrepancies.

(5) 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, and 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 Communications Authority.

(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 Communications Authority;
- 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 Certification-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 with electronic signatures 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 executed with electronic signatures 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 Communications Authority 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 Communications Authority 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 Communications Authority 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 Communications Authority shall be borne by the certification-service-provider terminating his activities.

(5) If a certification-service-provider has terminated activities and another service provider of higher level in that particular branch of service is not available in the Communications Authority's register, the Communications Authority shall retain the data and records specified in Subsection (6) of Section 9 and shall undertake the obligations referred to in Subsection (7) of Section 9.

(6) 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).

(7) The Communications Authority shall remove the certification-service-provider from the register if dissolved or if service activities are terminated.

## ***Feeding Signature-Creation Data into a Signature-Creation Device***

### *Section 16/A.*

(1) In this service, the service provider shall install the signature-creation-data of the recipient of the service on the signature-creation-device or shall personalize the signature-creation-device.

(2) The service provider shall provide for the safe generation of data used for the creation and verification of electronic signatures if data used for the creation and verification of electronic signatures are generated by the service provider on behalf of the recipient of the service.

(3) The service provider shall treat all signature-creation-data of the recipient of the service strictly confidentially, and it shall install safeguards so that they will not be compromised. The service provider shall not be authorized to store any signature-creation-data in a manner suitable to be retrieved during the life of the service and shall ensure that the signature-creation-data of the recipient of the service is not copied and stored following termination of the service.

(4) The service provider shall guarantee the safety of the signature-creation-device it provides.

(5) Service providers engaged in the installation of signature-creation-data shall be subject to the provisions pertaining to certification-service-providers with the exceptions set out in this Section.

## ***Time-Stamping Services***

### *Section 16/B.*

(1) The time-stamp created by a service provider shall provide a link between the current date and time (time data), the serial number and the electronic document to which the time-stamp is to be affixed or the image file of this document.

(2) The service provider shall only be allowed to alter the electronic document (or its image file) received from the recipient of the service for time-stamping to the extent necessary for time-stamping.

(3) Time-stamps and qualified time-stamps, and time-stamping service providers shall be subject, respectively, to the provisions pertaining to certificates and qualified certificates and to certification-service-providers with the exceptions set out in this Section.

## ***Electronic Archiving Services***

### *Section 16/C.*

(1) If so agreed by the parties, archiving services may be provided without the recipient of the service having to disclose his personal identification data to the service provider.

(2) Electronic-archiving-service-providers shall only be allowed to suspend the receipt of documents, or the image files of documents, for safekeeping; all other services must be provided without any interruption.

### *Section 16/D.*

Prior to contracting, the service provider shall inform the prospective client concerning the use of the service, the degree of security, the service procedures and the contract terms and conditions, and the applicable data protection regulations (in particular any access that may be open to persons other than the recipient of the service).

*Section 16/E.*

When accepting electronic documents executed with electronic signatures or image files, the service provider shall check the electronic signature and obtain the information necessary for the long-term use of the electronic signature, such as:

- a) information relating to the certificate, signature-verification-data, and information pertaining to the current status (revocation) of the certificate;
- b) in addition to what is contained in Paragraph a), the signature-verification-data of the service provider that issued the certificate and information on its revocation.

*Section 16/F.*

If information for the long-term use of the electronic signature is not available, the service provider shall so inform the recipient of the service without delay. The service provider shall be held liable under Section 16/M for any damages resulting from his failure to provide the above-specified information.

*Section 16/G.*

(1) When the information referred to in Section 16/E is obtained, the service provider shall affix to the validity chain a time-stamp issued by a qualified service provider, and it shall notify the recipient of the service accordingly.

(2) The service provider shall be required by order of the Communications Authority to affix to the validity chain a qualified electronic signature created on the basis of an approved cryptographic algorithm or a time-stamp issued by a qualified service provider:

- a) at the intervals specified in the service procedures;
- b) at the times specified by the Communications Authority.

(3) Upon receipt of the Communications Authority's decision, the service provider shall be required to affix to the validity chain a qualified electronic signature created on the basis of a cryptographic algorithm specified by the Communications Authority bearing specific parameters or a time-stamp issued by a qualified service provider by order of the Communications Authority.

(4) The service provider shall continuously monitor technical development in terms of electronic signatures and cryptographic algorithms, and if the Communications Authority has declared an approved cryptographic algorithm bearing specific parameters unsafe, the service provider shall affix to the validity chain a qualified electronic signature created on the basis of a safe cryptographic algorithm and a time-stamp issued by a qualified service provider, and it shall notify the Communications Authority accordingly. Within the meaning of this provision, a cryptographic algorithm shall be considered unsafe if - where used with specific parameters - signature-verification-data can be linked to signature-creation-data or if it allows the recreation of an electronic document from a particular image file.

*Section 16/H.*

The service provider shall safeguard the electronic documents executed with electronic signatures and image files entrusted to it by installing sufficient facilities to prevent the stored contents from being manipulated or corrupted, provide continuous access to authorized persons, and - if so prescribed in the service procedures - block all attempts to access these electronic documents executed with electronic signatures for reading. Electronic documents must be protected against unauthorized access, alteration, deletion and accidental destruction.

*Section 16/I.*

The contents of electronic documents executed with electronic signatures may only be read by the service provider or any person in the service provider's employ whether under contract of employment or in a self-employed capacity, upon the prior written consent of the recipient of the service.

*Section 16/J.*

The service provider shall ensure in accordance with the service contract that the recipient of the service has continuous access to his electronic documents.

## ***Data Processing by the Archiving-Service-Provider***

### *Section 16/K.*

The service contract shall contain sufficient facilities to comply with the requirements pertaining to data processing prescribed in the Personal Data Protection Act as concerning the personal data contained in the electronic documents.

## ***Obligations of the Recipient of the Service***

### *Section 16/L.*

If an electronic document is not part of the validity chain, the recipient of the service shall, unless otherwise prescribed in the service procedures, supply to the service provider - when requested at the intervals specified in the service procedures - an image file of the electronic document created on the basis of a cryptographic algorithm that has been approved by the Communications Authority. If the recipient of the service fails to comply with this obligation when requested, the service provider shall be relieved from the liability prescribed under Section 16/M.

## ***The Archiving-Service-Provider's Liability for Damages***

### *Section 16/M.*

(1) The service provider shall be held liable for any damage caused to other persons through damage to or destruction of the validity chain or the electronic documents and image files placed under his care. The service provider shall be relieved from liability if he can prove that the damage is the result of an unavoidable cause beyond his control.

(2) The service provider may install clauses in the service procedures to limit his liability for any damage caused to other persons through damage to or destruction of the validity chain or the electronic documents and image files placed under his care.

## ***Termination of Archiving Services***

### *Section 16/N.*

(1) If the service provider intends to terminate operations as well as in the cases defined in Subsections (2) and (3), the recipients of the service and the Communications Authority must be duly notified at least sixty days in advance.

(2) The service provider who is being wound up or liquidated shall immediately notify the Communications Authority to that effect and shall indicate the name of the proceeding agency. The Communications Authority shall be entitled to inquire at this agency concerning the status of the proceedings.

(3) The Communications Authority shall remove the service provider from the register if it is dissolved or its service activities are terminated.

### *Section 16/O.*

(1) Archiving-service-providers shall be subject to the provisions pertaining to certification-service-providers with the exceptions set out in Sections 16/C-16/N.

(2) The provisions pertaining to archiving-service-providers and to archiving services shall not concern the enforcement of the obligations set out in Section 12 of Act LXVI of 1995 on Public Documents, Public Archives and the Protection of Private Archive Materials.

## ***Responsibilities of the Communications Authority***

### *Section 17.*

- (1) The Communications Authority
  - 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 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 Communications Authority shall be governed by the Act on the General Rules of Administrative Proceedings and Services.
- (3)
- (4) The Communications Authority shall resolve all applications and petitions within sixty days from the date of receipt.
- (5) Appeals against the decisions on the first instance of the Office of the National Communications Authority may be addressed to the Chairman of the Council of the Communications Authority.
- (6) The Communications Authority may be assisted in its proceedings by judicial experts or other persons with expertise in electronic signature services registered under specific other legislation.
- (7) The Communications Authority's services in connection with registrations shall be subject to a fee, which is payable to the Communications Authority. The penalties levied under this Act shall be payable to the central budget.

## ***Technological Advance***

### *Section 18.*

The Communications Authority shall continuously monitor advancements in the technology related to electronic signatures and developments in cryptographic algorithms and shall adopt resolutions to define the cryptographic algorithms considered safe for use by the service providers and the requirements for their application with specific parameters. For the purposes of this Section, a cryptographic algorithm shall be considered safe if - where used with specific parameters - signature-verification-data cannot be linked to signature-creation-data or if it does not allow the recreation of an electronic document from a particular image file.

## ***Records and Directories***

### *Section 19.*

- The Communications Authority shall keep, and display, the following records and directories:
- a) Register of service providers registered according to Subsection (1) of Section 7, indicating the name, address (residence, business establishment, place of operation) of the service provider, description of the services provided and an indication that the service provider has been qualified for the service in question, the serial numbers of signature-creation-devices provided and any other data and information 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 systems of authentication and time-stamping to be issued by a qualified certification-service-provider, for which a code is assigned when registered.
  - e) the voluntary accreditation schemes referred to in Section 16/B and the bodies operating them, containing the

name of the voluntary accreditation scheme and the name and address (residence, business establishment, place of operation) of the person or entity in charge of operating it;

f) the service providers attested under a voluntary accreditation scheme referred to in Section 16/B, containing the name and address (residence, business establishment, place of operation) of the service provider and the name of the voluntary accreditation scheme, and the validity period attested.

## *Supervision of Service Providers, Measures*

### *Section 20.*

(1) The Communications Authority 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 Communications Authority shall be entitled to conduct on-site inspections upon providing proof of authorization. The Communications Authority'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 service provider. The service provider inspected shall cooperate to render the inspection possible.

(3) The Communications Authority shall conduct inspections of the following at qualified service providers within thirty days following the commencement of operations:

a) technical, safety and other operating and personnel requirements, in particular the criminal records and educational qualifications of employees and whether they are sustained on a continuous basis;

b) compliance with the relevant statutory provisions, the systems of authentication and time-stamping, service procedures, and with the general contract terms and conditions.

(4) The Communications Authority shall conduct comprehensive inspections at least once a year at qualified 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 Communications Authority's resolutions, and to prevent or terminate unlawful acts and discrepancies, the Communications Authority 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) delete from the register of service providers the designation of a service provider for being qualified with respect to a particular branch of service and forbid the service provider from using this designation;

g) remove the service provider from the register of service providers.

(2) The Communications Authority 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 service provider was subject to any disciplinary action in the past. Measures may be implemented individually or combined.

(3) The Communications Authority shall remove the service provider from the register 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 Communications Authority 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 Communications Authority shall concurrently implement the provisions laid down in Subsection (4) of Section 16.

(6) By order of the Communications Authority 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 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 Communications Authority's resolutions shall be subject to penalty. With regard to repeat offences, or if the certification-service-provider fails to carry out the Communications Authority'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 Communications Authority gains knowledge of the offence or breach of obligation, or after maximum three years from the date when committed.

(3) The Communications Authority 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.
- d) the archiving-service-provider fails to comply with the obligations specified under Sections 16/G-16/H.

(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 Communications Authority.

(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 Communications Authority 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 executed with electronic signatures produced subsequently and the electronic signatures by which these documents are executed. Subsection (1) of Section 3 and Subsection (7) of Section 5 shall also apply to the electronic documents executed with electronic signatures 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 Communications Authority 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 special requirements concerning electronic signatures that may be used in administrative proceedings and services, the certificates of electronic signatures and the related services provided in connection with electronic signatures with a view to the implementation of the provisions contained in Act CXL of 2004 on the General Rules of Administrative Proceedings and Services.

(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 Communications Authority under this Act for its services in agreement with the Minister of Finance.

d) - in agreement with the Minister in charge of the Prime Minister's Office, the Minister of the Interior, the Minister of Justice and the Minister of National Cultural Heritage - the regulations concerning copies made by way of electronic means under Subsection (8) of Section 4.

(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 documents executed with electronic signatures 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 documents executed with electronic signatures 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 documents executed with electronic signatures 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)

(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.*

*Section 31.*

*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 devices must not alter the electronic document to be signed to an extent beyond what is necessary for having the signature affixed, and they shall not prevent the signatory from exhibiting the document prior to the signature process.

### Schedule No. 2 to Act XXXV of 2001

Qualified certificates must contain:

- a) an indication that the certificate is issued as a qualified 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 qualified service providers***

Qualified 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 features 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) ensure that the signatory's signature-creation data are not recorded on the signature-creation device in the process of installing the signature-creation data;

k) before entering into a contractual relationship, inform the recipient of the service by proper means of the existence of a voluntary accreditation scheme and that the certificate or the service provided is qualified including the implications of this qualification, of the general terms and conditions and 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 document,
- 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.