The unofficial translation of Law No. 188(I)/2004 entitled Framework Law Providing for the Legal Framework for Electronic Signatures and Associated Matters of 2004, which was enacted by the House of Representatives of the Republic of Cyprus on 30 April 2004, is by Olga Georgiades of Lellos P. Demetriades Law Office. In translating the Cypriot law, Olga compared the English version of the EU Directive with the Greek text of the Law. Due to the fact that the EU Directive was largely transposed into Cypriot law, Olga used the official English version of the EU Directive to provide the English translation of the Cypriot law.

LAW No. 188(I)/2004

FRAMEWORK LAW PROVIDING FOR THE LEGAL FRAMEWORK FOR ELECTRONIC SIGNATURES AND ASSOCIATED MATTERS OF 2004

For the purpose of harmonisation with the act of the European Community entitled:

"Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19/01/2000 p. 12)";

The House of Representatives votes as follows:

Short title	1. This Law shall be referred to as the Law on the Legal Framework for Electronic Signatures and Associated Matters of 2004.
Interpretation	2. In this Law, unless the context requires otherwise,
Schedule I Schedule II	"qualified certificate" shall mean a certificate which meets the requirements laid down in Schedule I and is issued by a certification-service-provider who fulfils the requirements laid down in Schedule II;
	"Decision 2000/709/EC" shall mean Commission Decision of 6 November 2000 on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3(4) of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (OJ L 289, 16/11/2000 p. 42);
	"Competent Authority" shall mean the Minister of Commerce, Industry and Tourism;
	"secure-signature-creation device" shall mean a signature-creation device which meets the requirements laid down in Schedule III;
	"signature-creation data" shall mean unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;
	"signature-verification-data" shall mean data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;
	"signature-verification device" shall mean configured software or hardware used to implement the signature-verification-data;

	"signature-creation device" shall mean configured software or hardware used to implement the signature-creation data;
	"voluntary accreditation" shall mean any licence to certify electronic data, setting out rights and obligations governing the provision of certification services and which is granted by the Competent Authority upon request by the certification-service-provider concerned according to section 8;
	"Commission" shall mean the Commission of the European Communities;
	"electronic signature" shall mean data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;
	"member state" shall mean a member state of the European Union;
	"advanced electronic signature" shall mean an electronic signature which meets the following requirements: (a) It is uniquely linked to the signatory; (b) it is capable of identifying specifically and exclusive the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the said data is detectable;
	"certificate" shall mean an electronic attestation which links signature-verification data to a person who confirms his identity;
	"certification-service-provider" shall mean a legal or natural person or the provider who issues certificates or provides other services related to electronic signatures;
	"electronic-signature product" shall mean hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;
	"third country" shall mean a country that is not a member state;
	"signatory" shall mean a natural or legal person who holds a signature-creation device and acts either under his own name or on behalf of another natural or legal person or provider he represents;
Aim and scope of application	3. (1) This Law establishes the legal framework governing electronic signatures and certain certification-services for the purpose of facilitating the use of electronic signatures and their legal recognition.
	(2) This Law does not cover aspects related to the conclusion and validity of contracts

	or other legal obligations that are governed by the requirements as regards form and does not affect rules and limitations in relation to the use of documents provided by the applicable legislation in force.
Legal effects of electronic signatures	4. (1) An advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device shall have the same validity as a handwritten signature, both in substantial and procedural law.
	(2) The validity of an electronic signature and its admissibility as evidence is not precluded solely on the grounds that the conditions of the previous paragraph are not mutually present:
	Provided that, the legal effectiveness and admissibility of an electronic signature as evidence in legal proceedings shall not be not denied solely on the grounds that: (a) It is not in electronic form, or (b) It is not based upon a qualified certificate, or (c) It is not based upon a qualified certificate issued by an accredited certification-service-provider, or (d) It is not created by a secure signature-creation device.
Powers and functions of the Competent Authority	5. (1) Without prejudice to subsection (2), the Competent Authority shall exercise control over and ensure the effective application of this Law. The Competent Authority shall, in particular, have the power and function to: (a) supervise and monitor certification-service providers established in the Republic, as well as certification providers according to sections 6(2) and 8;
Schedule III	(b) monitor the compliance of signatures with the provisions of Schedule III; (c) may prescribe public or private providers for the purpose of certifying the compliance of secure-signature-creation devices with the provisions of Schedule III, according to section 6(2); (d) regulate voluntary accreditation according to the provisions of section 8.
	(3) Regulations issued under this Law may grant the Competent Authority more specific functions, powers, activities and duties facilitating the fulfilment of the aims of this Law.
Market access	6. (1) The provision of certification services originating from another Member State shall not be subject to limitations in the fields covered by this Law. Subject to section 8, there shall be no requirement for the granting of a licence to providers of certification services of any type.
	(2) The conformity of secure signature-creation-devices with the requirements laid down in Schedule III shall be determined by the Competent Authority or by public or private providers designated by the Competent Authority. The Competent Authority and the public or private providers designated by it shall be bound to apply the minimum requirements laid down by Decision 2000/709/EC. The conformity of electronic-signature products with recognized standards shall be deemed to be proof

	of compliance with the requirements prescribed in point (f) of Schedule II and with Schedule III.
	(3) Accredited or non-accredited certification service providers fulfilling the requirements of Schedule II shall issue qualified certificates to the public.
	(4) The electronic signature products that are provided may bear secure signature-devices and or non-secure signature-devices to the extent that this is set out in a manner that is absolutely clear for any third party, without prejudice to the provisions of section 5.
	(5) Verification certificates shall prescribe in an express manner and in a manner that is easily comprehensible by a third party who is not an expert whether they consist of qualified or non-qualified certificates.
Repetition (3) Schedule II	(6) Accredited or non-accredited certification service providers fulfilling the requirements of Schedule II shall issue qualified certificates to the public.
	(7) Electronic signature products that comply with the provisions of this Law shall circulate freely within the internal market.
	(8) Certification service providers must, in particular, ensure compliance with the provisions regarding the protection of competition, unfair competition, intellectual and industrial property and consumer protection.
	(9) The Competent Authority shall promote the development and use of the recommendations for secure signature-verification as laid down in Schedule IV and in the interests of the consumer.
Recognition of a signature originating in another member state.	7. If the Competent Authority of a member state has accredited the conformity of secure signature-creation-devices with the requirements laid down in Schedule III, then the signature shall be recognized within the Republic.
Voluntary accreditation	8. (1) In order to achieve an improved level of provision of certification services, the Competent Authority or the public or private providers appointed thereby, shall grant a voluntary accreditation, following an application in writing by the certification service provider concerned. The voluntary accreditation shall confer rights and shall impose obligations on the certification service provider, including charges that shall be prescribed by an Order.
	(2) The conditions of voluntary accreditation shall be prescribed by Regulations and must be objective, transparent, proportionate with the aims in question and non-discriminatory. The Competent Authority may not limit the number of certification service providers wishing to be accredited in accordance with the provisions of this Law.
Liability	9. (1) An accredited or non accredited certification-service-provider issuing a qualified certificate to the public or guaranteeing the accuracy of such certificate, shall be liable for damage caused to any entity or legal or natural person reasonably relying on that

	certificate, as regards: (a) the accuracy, at the time of issuance, of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate; (b) the assurance that, at the time of the issuance of the certificate, the signatory whose identity is confirmed in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate at the time of issuance; (c) the assurance that the signature-creation data as well as the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;
	(2) The certification-service-provider shall also be liable for damage caused to any entity or natural person who reasonably relies on the certificate if he fails to register the revocation of the certificate.
	(3) In all of the above cases prescribed in subsections (1) and (2), the provider shall not be liable if he proves that he has not acted negligently.
	(4) A certification-service-provider may indicate limitations in a qualified certificate on the use of that certificate, provided that the said limitations are recognisable by any third party. In this event, the certification-service-provider shall not be liable for damage arising from use of a qualified certificate that exceeds the limitations placed thereon.
	(5) A certification-service-provider may indicate in the qualified certificate limitations on the value of transactions for which the relevant certificate can be used, provided that these limitations are recognisable by any third party. In this event, the certification-service-provider shall not be liable for damage resulting from these maximum limitations being exceeded.
93(I) of 1996 69(I) of 1999	(6) The provisions of subsections (1) to (5) shall be without prejudice to the provisions of the Law on Unfair Terms in Consumer Contracts of 1996 to 1999, concerning unfair terms in consumer contracts.
International aspects	10. (1) The provision of certification services within the territory of the Republic by a certification service provider established in the Republic shall be subject to this Law.
	(2) Certification services provided by another member state in the fields covered by the laws of the European Union on electronic signatures, shall be legally equivalent to equivalent certificates issued by a certification-service-provider established in the Republic.
	(3) Electronic signature products complying with the laws of the European Union shall be legally equivalent to electronic signature products originating from the Republic. In particular, the verification of their compliance with the relevant legislation of the European Union concerning the requirements for secure signature-creation devices, by the provider who has been assigned with this verification according to the legislation

	of the member state of the European Union, shall have immediate effect in the Republic.
	(4) Qualified certificates issued to the public by a certification-service-provider established in a third country, shall be recognised as legally equivalent to certificates issued by a certification-service-provider established within the European Union, if: (a) The certification-service-provider fulfils the requirements laid down in this Law and has been accredited under a voluntary accreditation scheme established in a Member State; or (b) a certification-service-provider established within a member state and fulfilling the requirements laid down in the legislation of the European Union this Directive guarantees the particular certificate; or (c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the European Union and third countries or international organisations.
Data protection	11. (1) On the basis of the provisions of this Law, certification-service-providers, the competent Authority and all entities shall be subject to the Processing of Personal Data (Protection of the Person) Laws of 2001 to 2003.
	(2) In particular, the certification-service-provider issuing certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate: Provided that, the collection and processing of personal data for any other purposes shall be prohibited, except if the data subject has given his explicit consent.
	(3) Certification service providers shall be allowed to indicate in the certificate a pseudonym instead of the signatory's name.
Notification	12. The Competent Authority shall notify to the Commission and the other Member States on the application of the provisions of sections 6 to 8 and, in particular, it shall: (a) Notify information on national voluntary accreditation schemes, including any additional requirements pursuant to section 8; (b) notify the data, names and addresses of the national bodies responsible for accreditation and supervision, as well as of the bodies referred to in section 8; (c) notify the data, names and addresses of all accredited national certification service providers.
	(2) The Competent Authority shall notify the Commission as soon as possible, any changes in respect of the above information.
Offences and penalties	13. (1) Any certification service provider who:

	(a) is liable according to the provisions of section 10; (b) acts as an accredited certification service provider without being one; or (c) fails to comply with any order or mandate or decision imposed on him by the Competent Authority under this Law, the Regulations and Orders issued under it, shall be guilty of an offence and shall be liable, on conviction, to a penalty not exceeding 3.000 Cyprus pounds. In the event of a second or further conviction, the penalty may be doubled.
Power to issue Regulations	14. (1) The Council of Ministers shall have the power to issue Regulations prescribing the details concerning the exercise of the functions, powers and duties of the Competent Authority referred to section 4 and which concern the supervision of the implementation of the legal framework governing electronic signatures, the better implementation of the Law, as well as anything which must or should be regulated in this Law.
	(2) Without prejudice to the generality of subsection (1), Regulations issued under this Law may provide, in particular, for: (a) the conditions for voluntary certification; (b) the possible additional requirements subject to which electronic signatures in the public sector shall be used: Provided that, such requirements must be objective, transparent, proportionate and non-discriminatory, they shall relate only to the specific characteristics of the application concerned and must not constitute an obstacle to cross-border services for citizens.
Power to issue Orders	15. The Competent Authority shall have the power to issue Orders which may prescribe the technical procedures and the details on the exercise of the functions, powers and duties of the Competent Authority referred to in section 5 and concerning any issue regarding the monitoring of the legal framework governing electronic signatures and in particular regarding: (a) the determination of technical standards which shall apply from time to time; (b) the determination of the fees prescribed under section 8(1); (c) the amendment of the Schedules of this Law for the purpose of direct adjustment with the laws of the European Union.

SCHEDULE I
Applicable Requirements for qualified certificates

Qualified certificates must contain:

(a) an indication that the certificate is issued as a qualified certificate;

(b) the identification data of the certification-service-provider and the State in which it is established;

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

(d) a provision for a specific attribute of the signatory, to be included, if important, depending on the purpose for which the certificate is intended;

(e) signature-verification data which correspond 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;

(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; and

(j) limits on the value of transactions for which the certificate can be used, if applicable.

SCHEDULE II
Applicable Requirements for certification-service-providers issuing qualified certificates

Certification-service-providers must:

(a) Demonstrate the reliability necessary for providing certification services;

(b) ensure the operation of secure and immediate directory and revocation services;

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

(d) verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the person in the name of whom a qualified certificate has been issued;

(e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also use administrative and management procedures which are adequate and correspond to recognised standards;

(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the certification processes 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 so as to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

(i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings; such recording may be done by electronic means;

(j) not store or copy signature-creation data of the person to whom the certification-service-provider

provided key management services;

(k) before entering into a contractual relationship with a person seeking a certificate from them in order to support his electronic signature, to inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, the existence of a voluntary accreditation scheme and procedures for the submission of complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in an easily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on this certificate;

(l) use trustworthy systems to store certificates in a verifiable form, so that:

(i) only authorised persons can make entries and changes,
(ii) the authenticity of the information can be checked,
(iii) certificates are publicly available for retrieval only in those cases where the certificate-holder has given his consent, and
(iv) any technical changes compromising these security requirements are apparent to the operator.

SCHEDULE III
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, and that their secrecy is reasonably assured;

(b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived from elsewhere and that the signature is protected against forgery using currently available technology;

(c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against use by third parties.

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

SCHEDULE IV
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 data;

(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; and

(g) any security-relevant changes can be detected.