International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Electronic Commerce for Developing Countries (EC-DC)

Developing and least developed countries legal framework on e-commerce, digital signatures, e-certification, e-transactions, CAs and RAs
EC-DC project participant countries

Monday, February 26, 2001

Summary

María Gabriela Sarmiento. Project Administrative and Research Officer. ITU / BDT EC-DC project. Geneva – Switzerland. E-mail: ecdc@itu.int Fax: +41 22 730 54 84

The Americas Region

Country	Project of Law and/or Law (briefing)
Argentina	- Argentina imposes no import or domestic use controls on cryptography - Argentina has acceded to the Wassenaar Agreement and is committed to restricting the export of cryptographic products and technology as dual-use goods, including the new controls announced in December 1998. - On September 16, 1998, the United States authorized the export of unlimited strength encryption products (with or without key recovery) to the banking and financial, insurance, health and medical, and on-line electronic commercial sectors in Argentina. This is an indication that the U.S. has leveraged its authority to gain access to plain text information in those sectors within the country under Mutual Legal Assistance Treaty (MLAT)/Financial Action Task Force (FATF) provisions. <u>*ANTEPROYECTO DE LEY DE FIRMA DIGITAL*, BUENOS AIRES, 18 August 1999</u>: - Propose the recognition of digital signatures (public key) and the regulation by law of e-commerce, and e-payment. - Propose the creation of digital signature and e-messages, transaction at the Government's Level (e-government). - Propose the derogation of the mandatory requirement of having handwriting signatures. - Propose to follow the international standards – Use of private and public key (e.g. ITU-T X.509, PKCS, ANSI X9.31, ISO 9796). - Propose to eliminate the obstacles to digital signatures and promote the certification products and services in the country. - The project cites the UNCITRAL model law on e-commerce, the OECD, the WTO, and the American Bar Association work on this subject. - Propose the recognition of the CAs and its liability. - Indicates that any other formality - solemnity different from the signature stated by Law for the creation of a document shall be respected. (e.g. Notary) - Propose the issuance of Administrative acts with digital signatures. - Propose the recognition for the digital signatures of the same legal effects recognized for handwriting signatures. - Propose that the Courts consider documents issued with digital signature as evidence. - Propose that CAs will not need a license to provide certification services but the Project of Law will only regulate the licensed CAs. - Propose the recognition of certificates issued by CAs based within the MERCOSUR jurisdiction. The Parliament studied the proposal, which became Law and modified several provisions of other legal texts to avoid any contradiction between the Voted Law and precedent legal texts. The *Comisión Asesora para la Infraestructura de Firma Digital* and *SECRETARIA DE LA FUNCION PUBLICA*, dependiente de la *JEFATURA DE GABINETE DE MINISTROS* will control, regulate, the CAs, the digital signatures. <u>Decree Nº 427/98 from 16 April 1998 = *Firmas Digitales para la Administración Pública Nacional*</u>: - The Decree addresses the use of digital signatures by the public administration and sets requirements and conditions for the operation of a

	licensed CA in the digital-signature infrastructure of the public sector. - Digital signatures are recognised and can be used within the National Public Administration for internal use only. (Its enforcement and validity are regulated). - This technology will be used for the implementation of the internal activities of the National Public Sector, which do not individually and directly generate legal effects. Under the present Decree, the digital signature will have the same value as the holograph signature only for internal acts. - The relationship between a public key -one of the pair of keys that allows the verification of a digital signature- and its holder will be guaranteed by a public key certificate issued by a Licensed Certification Authority. - The requirements and conditions for the life cycle and validity of the public key certificates (issuing, acceptance, revocation, expiration, and other contingencies of the procedure), as well as the conditions for the operation of the Licensed Certification Authorities are regulated in this decree. - The Civil Service Administration Secretariat, reporting to the Ministerial Chiefs of Cabinet, will be the Implementing Authority for the present Decree and will carry out the functions of Licensing Institution. - The National Accountant General's Office, reporting to the Budget Undersecretary's Office of the Finance Secretariat of the Ministry of Economy, Public Works and Services will undertake the functions of Auditing Institution. Other legal texts related to digital signatures (e.g. resolutions): - Resolution MTSS N° 555/97 from *MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL (Normas y procedimientos para la incorporación de Documentos y Firma Digital);* - Resolution SAFJP Nº 293/97 from *SUPERINTENDENCIA DE ADMINISTRADORAS DE FONDOS DE JUBILACION Y PENSIONES (Incorporación del Correo Electrónico con Firma Digital);* - Resolution SFP Nº 45/97 with respect to the application of digital signatures within the public administration for the promotion and dissemination of the digital document and signature was issued from March 17 1997. SECRETARIA DE LA FUNCION PUBLICA (Incorporación de Tecnología de Firma Digital a los Procesos de Información del Sector Público). The Resolution allows the use of digital signatures in the public sector in accordance with the Conclusions of the Subcommittee on Cryptography and Digital Signatures on the Technical Guidelines Regarding Digital Signature Standards (30 December 1996). - Resolution SFP Nº 194/98 from the *SECRETARIA DE LA FUNCION PUBLICA (Estándares Aplicables a la Infraestructura de Firma Digital para el Sector Público Nacional del Decreto Nº 427/98);* - Resolution SFP Nº 212/97 from the *SECRETARIA DE LA FUNCION PUBLICA (Políticas de Certificación para el Licenciamiento de Autoridades Certificantes).*
Brazil	- There is a certification hosted at www.certisign.com.br In 1999, there were some bills in this matter discussed in the Congress. - For CAs there is industry self-regulation, with government intervention only in cases of major abuse or neglect. - For Brazil, CAs shall be established on a national level by national authorities. - Some informal industries standards, loosely defined under the law have become CAs in Brazil. *PROJETO NA CASA DE ORIGEM (CÂMARA DOS DEPUTADOS) - Sala das Sessões*, 31 August 1999. A Special Committee of the Brazilian House of Representatives is finalizing a Bill of Law to govern e-commerce transactions in Brazil. It is based on the UNCITRAL Model Law. It establishes the minimum requisites of security and certification for electronic signatures and documents. Electronic certification activities will not be exclusively

	performed by Public Notaries, as contemplated in the in the original draft of the Bill. E-transactions are fully recognised. Briefed description of the content of the project: - E-Public Procurement or e-government is recognized. - E-documents and messages are recognized legal effects. - Digital signatures are recognized. - Public key certifications are recognized. - Public and private e-certificates are recognized. - RAs and CAs are recognized. - *Do Ministério da Ciência e Tecnología* regulates and control the RA and CAs. - Foreign certificates are recognized. *PROJETO NA CASA DE ORIGEM (SENADO FEDERAL)* - 13/12/99: The same as in the Chamber of Deputies, plus: - E-contracts are recognized (validity, legal effects, etc).
Chile	- There are reportedly no prohibitions on the export, import, or domestic use of cryptographic products in Chile. *PROYECTO DE LEY SOBRE DOCUMENTOS ELECTRÓNICOS* (Presented to the Parliament on 9th August 2000): - Recognition of e-documents. (validity, legal effects, enforcement, etc). - A document signed with a digital signature is recognised and produce legal effects if some requirements are duly filled. (Article 4) - Digital signature shall be created with the public key method (public and private keys). - An e-document shall be considered as The original if some requirements are fulfilled (Article 5) - Notaries can undertake their responsibilities by electronic means. - Recognition of e-transactions. - CAs are recognized, but only Notaries and its equivalent can become CAs. - Certificates are recognized - Third parties (legal or physical person) who can have a database and act as intermediaries between the certified person and the public shall be registered. - The *Instituto Nacional de Normalización* (INN) is the competent authority to adapt, recognise, and apevidence new standards, formats, etc on e-documents. - E-documents can be presented to the Courts as evidence.

Colombia	Law No. 527 from 18th August 1999: The law is based on the UNCITRAL Model Law on Electronic Commerce: - Recognises and regulates the Electronic data Interchange (EDI) and other information sent electronically (e.g. Internet, e-mail). - Gives legal recognition to all kind of e-information - Recognises an electronic document as a written document. - E-signatures are recognized only if the person can be identified and the content and integrity of the document can be controlled. It is also necessary that the way the signature is created is safe. - Recognises an electronic document, message as the original only if the integrity of the document is evidenced and if the document or message can be showed upon request. - E-documents and e-messages are admitted as evidences at a court. - Offer and acceptation can be provided by electronic means. - E-contracts are recognized. - Any agreement, declaration, wills, etc. expressed by electronic means is valid. - Electronic contracts related to transportation of merchandise are recognized. - Transportation documents can be delivered electronically (e.g. bill of landing) - Digital signatures have the same legal effects as the handwriting signature only if some requirements are duly filled. (Article 28) - National or Foreign, Public and Private Legal persons can become a CA, also the Chamber of Commerce can be a CA only if they are authorized by the *Superintendencia de Industria y Comercio* and fulfill the National Government's requirements. (Article 29) - CA can deliver certificates related to the digital signature of legal and physical persons, related to the content and integrity of electronic messages (verification). - CA can provide certified digital signature services, registration services, timing, transmission and reception of electronic messages, database services, etc. - CAs and certificates are regulated by this Law (revocation, requirements, etc.) - Certificates issued by a foreign CA are recognized. Decree No. 1747 from 11th September 2000 por el cual se reglamenta parcialmente la Ley 527, en lo que respecta las entidades de certificación, los certificados y las firmas digitales: - The Decree regulates all related issues to certification authorities (operation, insurance, infrastructure, resources, etc.) and digital certificates. - For the decree there are to types of CAs, the open CAs and the closed CAs. - National CAs can recognise foreign digital signature certificates. - The certification system will be considered as a secure system only if it fulfills the standards established by the *Superintendencia de Industria y Comercio*.

	Resolution N° 26.930 from 26th October 2000 por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores: - The resolution regulates the open and closed CAs. It also regulates the auditing institutions to the CAs, the certificates, and the certification practices.
Cuba	Participant's information: - There is a Cuba's current legislation on data protection. Cuba signed an agreement to approve the Model Law project on data protection that has been taken into account for the draft of Cuba's law. - Cuba is working on an ecommerce law taking the UNCITRAL Model Law on ecommerce as example. Cuba is currently working on the Contracts Law Project, which regulates econtracts. For now, the Civil Code (Law 59 from 16 July 1987) is applicable to these cases. A proposal has been introduced to the Commission in order to update the civil code provisions regarding the e-commerce requirements. - A draft of a digital signature act has been presented to the Commission. - A draft of a Law regulating the CAs and RAs has also been presented to the Commission. It aims to establish the use and rules to run and operate CAs and RAs and to institutionalize them. - The Law-Decree 199 from 25 November 1999 has established the rules for the design, import and commercialization of encrypted technology.
Dominica	- There are no domestic use prohibitions, export or import controls on cryptography in Dominica. - On September 16, 1998, the United States authorized the export of unlimited strength encryption products (with or without key recovery) to the banking and financial, insurance, health and medical, and on-line electronic commercial sectors in Dominica. This is an indication that the U.S. has leveraged its authority to gain access to plain text information in those sectors within the country under Mutual Legal Assistance Treaty (MLAT)/Financial Action Task Force (FATF) provisions.
Ecuador	*PROYECTO DE LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS* - Ecuador Law Governing Electronic Commerce, Electronic Signatures, and Data Messages: - Establishes the validity and enforceability of electronic signatures, as well as "data messages." Its information and content have legal validity as public and private documents. - Recognises the cryptography. - Recognises e-commerce. - States Confidentiality, and Data protection provisions. - When a written text is required, the data message will be valid as a written text if it can be consulted in the future. - When the original document is required, the data message will be considered as the original if the integrity of its content is guaranteed. - When some documents, registrations or other information must be kept, the data message that has been kept will fulfill the requirement. - When a signature is required, a digital signature will fulfill the requirement if a safe method has been used and the undersigned can be identified.

	The electronic signature shall have equivalent validity, and shall be recognized to have the same legal effects, as a handwritten signature. - The digital signature has the same legal validity and effects as a handwriting signature, if some requirements are fulfilled. (Article 12 - 13) - The digital signature is par of the data message. - Recognises e-contracts. They are enforceable. For all purposes, e-contracts will have the same effects that the law attributes to signed documents. Regulates e-contracts formation, offer, acceptation, reception, and conclusion. - Recognises the certification of digital signatures. The certificates shall have full effect before government and private agencies and may contain additional attributes as specified by law. Regulates the duration (validity), suspension, cancellation, and revocation of digital signatures. - Recognises the Certification Services Providers (CSPs). The Law states the duties of CPS who must be accredited. An individual or a legal entity that is legally competent to issue certificates of identity and provide services related to electronic commerce and signatures, and for which purpose it is able to comply with requirements set by law and regulations by means of the necessary physical and logical tools compatible with the type of service to be offered. - The *Superintendencia de Telecomunicaciones* is the organ that will control, accredit and sanction the CSPs. - Regulates the CSPs database use and management. - Written documents that have been transferred into e-documents in presence of a Notary will be considered as authentic copies. - Data message can be used as evidence at the Courts. The data message, whatever its source or generation, shall be considered a means of evidence with all legal effects that principals of evidence have under the Code of Civil Procedure and under the Code of Penal Procedure. - The Bill addresses the use of electronic public documents. Electronic Public Validators shall meet the same requirements as certification service providers. Written documents that are converted into electronic documents in the presence of a notary shall be considered authentic electronic copies. The same applies in the reverse situation. Electronic documents issued by a notary or competent authority and signed electronically by them have the same legal effects as written documents of the same type.
El Salvador	- By 1999, no specific legislative or regulatory effort was undertaken to adapt national contract law to account for the new challenges posed by electronic transactions. - By 1999, the legislation did not mention the acceptance/recognition of digital signatures. Digital signatures are used in practice; however, a written document is needed for support.
Mexico	- There are no domestic controls on the use of encryption in Mexico. - There are no export or import restrictions on encryption technology. - There are some government requirements and licensing of private CA's. - Mexico considers that CAs shall be established at national and international levels. - There are government established and operated Certification Authorities. *DICTAMEN DE LAS COMISIONES UNIDAS DE JUSTICIA Y DE COMERCIO, CON PROYECTO DE DECRETO POR EL QUE SE DICTAMINAN DIVERSAS REFORMAS Y ADICIONES AL CODIGO CIVIL FEDERAL, AL CODIGO DE COMERCIO Y A LA LEY FEDERAL DE PROTECCION AL CONSUMIDOR EN MATERIA DE COMERCIO ELECTRONICO:*

	- Propose to follow the guidelines of the UNCITRAL model law on e-commerce, - Propose to modify the Civil Code and include the legal definition of electronic data message. - Propose the recognition of e-contracts, offer, and acceptation, and enforceability. - Propose data messages to be considered as a written text. - Propose to provide validity and legal effects to data messages and that they can be considered as evidence at a Court. - Propose the recognition of digital signatures for public services. - Propose to identify the sender of a data message by mean of a password or code. - Propose the recognition of data messages and other e-information as evidence at a Court. - Propose the Commercial Public Registry to act as verification authority. The registry shall keep a database, etc. On May 29, 2000, the long awaited amendments to the Civil and Commercial Codes (here-above) that set the ground for electronic transactions in Mexico were finally published in the Official Gazette. These amendments, that follow the UNCITRAL model law, will enter into force next June 7th. The enactment amended the Federal Civil Code ("CC"), the Federal Commercial Code ("CCom"), the Federal Civil Procedures Code ("CPC") and the Federal Consumers' Protection Law ("CPL"). - Parties can enter into an agreement, whether explicit or tacit, in addition to the formerly recognized manners, by expressing their agreement by electronic means (e.g., an "I Accept" click), providing that the assent by electronic means should be considered as clear manifestation of the party's desire to enter into an enforceable agreement. - Substantial amendments in the CPC and CCom provide that all kinds of information generated from technological means (electronic, optic, and any other kind of technology) will be considered valid evidence. - The amendments significantly emphasize that agreements entered into through technological means and in general, technological resources, will only be valid when they comply with the Evidentiary Requirements. - Elimination of the need of prior written agreements. - As with the CC, the amendments to the CCom begin by recognizing that technological means as acceptable for entering into valid binding agreements. - The amendment also sets forth the basis for implementing the use of information technology in the Registry's operations.
Panama	The Secretaria Nacional de Ciencia y Técnica e Innovación (SENACYT) will present an Anteproyecto de Ley de Certificación de Firma Digital y Comercio Electrónico in Panama: - Propose the recognition and enforcement of e-transactions, e-agreements, e-conventions, etc. - Propose the recognition of the digital signature e-certificate and promotes the digital signature certification services. - An e-commerce centre has been created to provide certification services to guarantee e-transaction for the public and private sectors. - Propose the creation of a CA. - Propose the recognition of Certification private companies.

Peru	*LEY DE FIRMAS Y CERTIFICADOS DIGITALES* (Law No. 27.269 from 26th May 2000): - Digital signatures are recognised and have the same legal effects as the handwriting signatures. - The recognized digital signature is the one which is part of the electronic message that identifies the sender of the message, and can provide authentication and integrity of the content of the message. - The method for the digital signature shall be the asymmetric cryptography (public and private keys) - Digital certificates issued by a CA are recognised. See requirements, revocation, etc. - Certificates issued by a foreign CA are recognized. - CAs issue and revoke digital certificates and provide services related to the certificates and, in general, to e-commerce. - CAs can also provide the Registration and Verification authorities services. - The competent authority (to be defined by decree) will register the CAs, RAs, and Verification Authorities (VAs). - The competent authorities can apevidence the use of a different technology for creation of digital signatures.
Trinidad & Tobago	- By 1999, a policy review on the legal treatment of contractual issues in e-commerce was underway. - There are government guidelines and general oversight of private CA's. There is also industry self-regulation, with government intervention only in cases of major abuse or neglect. - For Trinidad and Tobago, CAs shall be established at national and international levels. - By 1999, there were no significant initiatives concerning the establishment of CAs.
Uruguay	- According to articles 129 and 130 of Law No. 16002 of 1988, all government documents transmitted electronically are considered 'authentic' for any legal purpose and those who transmit false documents may be prosecuted. In 1995, articles 694 to 698 of the five-year national budget law (No. 16736) extended the application to all documents. - There is no specific law on digital signatures. - On account of their reputation as trusted third parties, both Uruguay's Post Office and the Chamber of Commerce and Services are entitled to certify the identity of the signer of an electronic document by means of an asymmetric code registry. - There are reportedly no export, import, or domestic use controls on cryptography in Uruguay. - On September 16, 1998, the United States authorized the export of unlimited strength encryption products (with or without key recovery) to the banking and financial, insurance, health and medical, and on-line electronic commercial sectors in Uruguay. This is an indication that the U.S. has leveraged its authority to gain access to plain text information in those sectors within the country under Mutual Legal Assistance Treaty (MLAT)/Financial Action Task Force (FATF) provisions.
Venezuela	*PROYECTO DE LEY DE RECONOCIMIENTO LEGAL DE MENSAJES DE DATOS Y FIRMAS ELECTRÓNICAS:* - Recognises the efficacy and legal validity of digital signatures and any electronic message, electronic information, etc.

	- Recognises and regulates de CAs and the electronic certificates. - Recognises data messages legal effects. They can be presented as evidence at the Courts. The electronic format of a data message is as valid as the stamped copy of the document. - Recommends that the Government adopt the necessary measures to develop the public organ functions by electronic means. - The digital signature certified by a CA is as valid as a handwriting signature. - Data messages can be considered as the original document if some requirements are fulfilled (Article 8). - When written documents are required, the validation is fulfilled with the presentation of a data message. - Recognises e-contracts and regulates its formation, validation, offer, acceptation, reception, etc. - E-contracts, any legal act contained in data messages, digital signatures and e-certificates can be considered as evidences at a Court. - The digital signature has the same legal effects as the handwriting signature. - Only digital signatures certified by a CA produce legal effects. - Regulates the validity, revocation, and suspension of digital signatures. - Foreign or national, public or private, legal or physical persons can become CAs. Also, other associations or chambers can be CAs. - CAs shall subscribe to the competent public organ (To be defined). - Recognises e-certificates for digital signatures for private or public, legal or physical persons. - CA shall provide certification services, creation of digital signatures, and a chronological database of certified digital signatures. - CAs can stop its activities with a previous authorization from the competent public organ. - E-certificates provide authenticity and integrity to digital signatures. - Regulates the revocation of e-certificates. - CAs will be supervised by a *Dirección General de* _____ *del Ministerio de* _____. - Regulates de suspension and revocation of the authorization for a CA to exercise its activities.

Asia & Pacific Region

Country	Project of Law and/or Law briefing
Bhutan	- By 1999, no specific legislative or regulatory effort was undertaken to adapt national contract law to account for the new challenges posed by electronic transactions.
Cambodia	- By 1999, no specific legislative or regulatory effort was undertaken to adapt national contract law to account for the new challenges posed by electronic transactions. - There are government requirement s and licensing of private CAs. - For Cambodia CA's shall be established at national and international levels. - There are no significant initiatives regarding established CAs. Participant's information: - The Government of Cambodia is forming an Electronic Transaction Act using the Singapore Electronic Transaction Act as a model. It is expected that the new Sub-decree (a temporary step towards a full act) will be available by June 2001. The Sub-decree will regulate CAs and RAs. - There are no restrictions for import or export of encryption technologies, or domestic controls on the use of encryption technology for civilian use. - There is no limitation on the encryption key size authorized for civilian use. - Electronic data, message, information and other can be presented as evidence at a Court. - Private companies cannot yet operate as CAs and/or RAs. Initially, the government should run and operate CA's. Later, the private sector may do so. CAs should not necessarily be established at a national level in each country. CAs and RAs shall be authorized by the Authorities to provide certification, verification and registration services.
China	- An E-commerce Certificate Authentication Centre has been established in Shenzhen to provide authentication of network identities, with the aim of protecting against online theft and guaranteeing the security of e-commerce. - In March 2000, the State Encryption Management Commission issued a notice on Questions Concerning the Administration of Commercial Encryption to US businesses, clarifying rules that had previously sent jitters through the foreign business community. The March notice further explained that the Draconian encryption rules would be targeted only at software solely aimed at encoding and decoding data. - With amendments to the Contract Law in force since October 1st 1999, contracts entered into on the Internet have been given the force of law. To meet needs before a more complete regulatory environment for e-commerce is established, the central bank has set up the Finance Certification Policy and Management Direction, charged with helping to settle disputes arising from e-commerce. - The importation, distribution and use of commercial encryption products in China is regulated by the State Encryption Management Commission ("SEMC") under the Chinese Encryption Regulations that went into effect on October 7, 1999 - Only foreign owned entities in China may import and use commercial encryption products developed outside of China: a. To import and use such foreign-developed commercial encryption products, the foreign-owned entity must obtain prior approval from the SEMC and b. Failure to obtain the requisite approval may result in: (1) Seizure of the foreign commercial encryption products; and (2) Fines of up to 3 times the value of the

	products, or 3 times any commercial gain from the importation and use of the products. - Chinese entities are required to use only domestically developed encryption products, and the distribution to, or use by, Chinese entities of foreign commercial encryption products is prohibited: A distributor of domestic commercial encryption products in China must have a "Commercial Encryption Product Sales Permit" issued by the SEMC, and must report each sale of commercial encryption products to the SEMC, including the following information: The name and address of the end-user; the institution code or identity card number of the end-user; the end-user's stated end-use of the product; and all current Chinese users of encryption products were required to register with the SEMC by January 31, 2000. - Pursuant to a Notice issued by the SEMC on March 10, 2000, called the "Circular on the Relevant Questions on Administration of Commercial Encryption Products", the SEMC apparently intends to apply the limitations and restrictions of the October 7, 1999 Encryption Regulations solely to those products which incorporate encryption and decryption operations as their core functions.
Hong-Kong	- The importation of encryption products into Hong Kong is subject to regulation by the Hong Kong Trade Department. - The import licensing requirements for encryption products in Hong Kong is tied to Hong Kong's implementation the Wassenaar export control program (primarily to prevent unauthorized diversion to China): a. As a general matter, a license from the Trade Department is required for the import of encryption products with an encryption key greater than 56 bits DES or 512 bits RSA, unless the product is a "mass market" encryption product with an encryption key length of 64 bits or less. - Importation of controlled encryption products into Hong Kong without the requisite import license is subject to fines of up to HK $500,000 and imprisonment for up to 2 years, upon summary conviction. - The Legislative Council enacted the Electronic Transactions Ordinance (Cap 553 - ORDINANCE NO. 1 OF 2000) in January 2000 to foster the development of e-commerce in Hong Kong. The new law gives electronic commerce and digital signatures used in electronic transactions the same legal status as their paper-based counterparts. Through the use of public and private key pairs and recognised certificates, individuals and businesses can, under the law, establish the identity of opposite parties in electronic transactions, ensure the integrity of the electronic messages received and prevent electronic transactions from being repudiated. Section 34 of the law appointed the Postmaster General as a certification authority (CA). The law also outlines the procedures for government recognition of other CAs and the certificates they would issue. On 7 January 2000 the Legislative Council has enacted the Electronic Transactions Ordinance: - If a rule of law requires information to be or given in writing or provides for certain consequences if it is not, an electronic record satisfies the requirement if the information contained in the electronic record is accessible so as to be usable for subsequent reference. - Where a rule of law requires that certain information be presented or retained in its original form, the requirement is satisfied by presenting or retaining the information in the form of electronic records, by fulfilling some requirements. (Section 7) - Under the Electronic Transactions Ordinance passed in Hong Kong in January parties to an e-commerce transaction may be identified through the use of public and private key pairs and recognized certificates. - If a rule of law requires a signature, a digital signature of the person satisfies the requirement but only if the digital signature is supported by a recognized certificate and is generated within the validity of that certificate. - Contracts concluded by electronic means are as valid as written contracts. The Ordinance regulates the offer and acceptance of the contract. - An electronic record shall not be denied admissibility in evidence in any legal proceeding on the sole ground that it is an electronic record. - A certification authority may apply to the Director of Information Technology Services to become a recognized certification authority for the purposes of the Ordinance. The Director may recognize certificates issued by a recognized certification authority as recognized certificates, upon

	application by that authority. (See also revocation and suspension – Sections 23 to 26). - The Postmaster General is a recognized CA and may perform functions and provide services of certification authority.
India	The government has passed the Information Technology Bill (ITB) on June 16th 2000 which came into force in October 2000. The bill gives legal recognition to digital signatures and outlines the penalties and procedures for dealing with cyber crimes. - The Information Technology Bill, seeks to 'provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce', which involves the use of alternatives to paper-based methods of communication and storage of information, [and] to facilitate electronic filing of documents with government agencies.' It establishes the legal validity and enforceability of digital signatures and electronic records, as well as secure digital signatures and secure electronic records. For additional information, see the Baker & McKenzie website. - The ITB provides for digital signature (secure and unreliable), public and private key, digital certificate, certification authorities, and recognition of foreign specified certification authorities. The ITB also lays down the duties of certification authorities, limitation of liabilities of certification authorities, and framework for regulation of certification authorities that includes appointment of controller of certification authorities, etc. - The ITB deals with the issues of validity of online contracts in the same way as the Model Law. Unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of "electronic records". - The ITB states that where a law requires information to be written or to be presented in writing or provides for certain consequences if it is not, an electronic record satisfies that rule if the information contained therein is accessible so as to be usable for subsequent reference. - The Government has announced that it plans to appoint certifying agencies who will issue digital signature certificates and will be responsible for the security of online transactions. - The Indian Contract Act allows for certain contracts to be made in forms other than in writing. Hence, online contracts may be valid as they may be considered to be in these other forms, but there are problems concerning the validity of contracts that need to be in writing. Indian law prescribes some contracts to be in writing. Therefore, it is possible that where the law does not prescribe contracts to be made in written form, contracts can be made in other forms. Oral contracts are thus valid and online contracts can also be subsumed under the rubric of other forms. The Indian Contract Act regulates the offer, acceptance, revocation of the offer and acceptance, etc. - There is a need to understand the difference between normal contracts and online contracts, especially with respect to the question of where and when the contract is concluded. In this connection, the paper discusses dispatch and receipt of data messages with reference to the UNCITRAL Model Law and the Information Technology Bill, 1998 and compares it with offer and acceptance under Indian law. - The Indian Evidence Act requires documents to be proved by primary evidence, and the validity of data messages as primary evidence is uncertain. There is an allied discussion on how to adduce information stored in computers. - There are several legislations, which require written documents. Printouts from information stored on computer may be regarded as "writing". As of today, it is unclear whether this interpretation is valid or not. - By 1999, there was no law regulating encryption. The Department of Telecommunication ("DoT") controls all aspects regarding Tele-communications, including encryption. As of today, permission is required from the DoT to send encrypted messages.
Iran	- As e-commerce has yet to hit Iran, this is not yet an issue. - See THE WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS, DUAL-USE GOODS, AND TECHNOLOGIES

	LIST OF DUAL-USE GOODS AND TECHNOLOGIES AND MUNITIONS LIST. 03-12-98.
Malaysia	The Digital Signature Act, passed in April 1997 and went in to effect on October 1st 1998, provides for, and regulates use of, digital signatures (high-tech electronic authorisation codes). In the area of certifications, which are used to verify the authenticity of a specific website, individual or company on the Internet, Digicert is Malaysia's only licensed certification authority that offers digital certificates to individuals and organisations. Digicert provides two types of digital certifications——a personal certificate which verifies the identity of an individual, and a server certificate which guarantees the authenticity of a specific website. For a detailed summary of the Digital Signature Bill go to the Baker & McKenzie web site (http://www.bmck.com/ecommerce/malaysia.htm - 22). Participant's information: - There are two phases to the registration: one to register as a licensed Certification Authority and the second to apply for a license to operate. The process for registration is the same for both local and foreign CAs. It could take a year to register as a CA. A Registration Authority currently does not need to be registered with the Malaysian Controller nor does he need a license to operate. - This bill establishes the legal validity, enforceability and admissibility of digital signatures. It recognizes repositories and authorizes the Minister to appoint the Controller of Certification Authorities. - It addresses the functions of certification authorities, the general requirements for a licensed certification authority, and the application procedures to become a licensed certification authority. - It also subjects the licensed certification authorities to annual performance audits. - It delineates requirements for the issuance, suspension and revocation of a certificate. - Where a rule of law requires a signature or provides for certain consequences in the absence of a signature, that rule shall be satisfied by a digital signature after fulfillment of some requirements stated in article 62 of the Digital Signature Bill. - Notwithstanding any written law to the contrary: a document signed with a digital signature in accordance with this Act shall be as legally binding as a document signed with a handwritten signature, an affixed thumb-print or any other mark; and a digital signature created in accordance with this Act shall be deemed to be a legally binding signature. - A message shall be as valid, enforceable and effective as if it had been written on paper if it bears in its entirety a digital signature; and that digital signature is verified by the public key listed in a certificate which, was issued by a licensed certification authority; and was valid at the time the digital signature was created. - A copy of a digitally signed message shall be as valid, enforceable and effective as the original of the message unless it is evident that the signer designated an instance of the digitally signed message to be a unique original, in which case only that instance constitutes the valid, enforceable and effective message. - There are no export, import or domestic use controls on cryptography in Malaysia. - MIMOS, a non-profit and government-owned company, has started the provision of the first public key certification services as mTRUST.
Mongolia	- There are import controls and domestic use controls on cryptography. Cryptography may only be used by lawful enterprises approved by the National Security Board.

Nepal	Participant's information: - The Information Technology Bill 2000 has been submitted in Parliament for ratification and recognition of digital signatures. - There are no restrictions for import/export from encryption technologies in the drafted law. - Currently there is no limitation on the encryption key size authorized for civilian use. - The drafted law indicates the use of encryption technology. His Majesty of Government is quite positive for e-commerce development. - Electronic data, message, information and other can be presented as evidence to a Court. - Only non-profit organizations (e.g. chambers) will get authority to run and operate as CA's and RA's upon obtaining license from the Government. This is indicated in the drafted legislation. Government will take full authority and delegate its power to the private sector. - Presently there is no legislation on CA's and RA's. - CA's should be established at a national level in each country.
Pakistan	- Given the extremely low value of e-commerce in the country, the government has not decided on strategies to deal with the Internet. - All encryption hardware and software must be inspected and authorized by the Pakistan Telecommunications Authority (PTA) before sale and use. Algorithms and keys must be inspected and deposited with the PTA. The governing law is the Pakistan Telecommunication (Reorganization) Act. Pakistan also severely restricts the use of voice encryption used in cellular networks.
Philippines	- The use of cryptographic hardware and software is not currently controlled in the Philippines. - Concerning the CA's the industry has its self-regulation, with government intervention only in cases of major abuse or neglect. - For Philippines CA's shall be established at national and international levels. - Some industry standards, loosely defined under the law have become CAs. - The law prescribes penalties for computer hacking: a minimum fine of P100,000 and maximum fine commensurate to damages incurred, and imprisonment of between six months and three years. The same penalties are prescribed by the law for piracy, or the unauthorized copying, reproduction, distribution and downloading of electronic signatures or copyrighted works on the Internet. The Philippine Congress passed the Electronic Commerce Act of 2000 (Republic Act 8,792) in June, providing the legal framework for e-commerce: - The law recognises digital signatures as legally binding in private online contracts, and allows the legal retention of these documents. It also mandates state agencies to establish processes and procedures that will allow government permits to be granted online, eradicating bureaucratic red tape. - An electronic signature on the electronic document shall be equivalent to the signature of a person on a written document if that signature is proved by showing that a prescribed procedure, not alterable by the parties interested in the electronic document. - Electronic documents shall have the legal effect, validity or enforceability as any other document or legal writing. Where the law requires information to be presented or retained in its original form, that requirement is met by an electronic data message or electronic document if some requirements are fulfilled. (See Section 10). - Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the data message purporting to give rise to

	such legal effect, or that it is merely referred to in that electronic data message. As between the originator and the addressee of a electronic data message or electronic document, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of a electronic data message. - The Act regulates the formation and validity of electronic contracts. - Government can use electronic data messages, electronic documents and electronic signatures. - The Act regulates the acknowledgment of receipt, the dispatch and the reception of electronic data messages or electronic documents - The Law makes electronic documents admissible as evidence in court. In any legal proceedings, nothing in the application of the rules on evidence shall deny the admissibility of an electronic data message or electronic document in evidence.
Singapore	- There are some government requirements and licensing of private CA's (voluntary licensing with guidelines) - For Singapore CAs shall be established at national and international levels. Regarding the CAs, existing industry-based private authorities, under governments guidelines operate in Singapore. - Until this year, an import permit from the Singapore Trade Development Board was required for the import of encryption products into Singapore. By regulatory amendments dated January 21, 2000, however, the Singapore Info-Communications Development Authority and the Trade Development Board eliminated those import permit requirements for encryption products, as part of Singapore's overall strategy to become a major information technology and e-commerce hub for the Asia/Pacific region The Electronic Transactions Act of 1998 established the validity of digital signatures in legal transactions. For a fuller discussion of the legislation see the Baker & McKenzie web site (http://www.bmck.com/ecommerce/singapore.htm#eta): - Information shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record. - Where a rule of law requires information to be written, in writing, to be presented in writing or provides for certain consequences if it is not, an electronic record satisfies that rule of law if the information contained therein is accessible so as to be usable for subsequent reference. - Where a rule of law requires a signature, an electronic signature satisfies that rule of law. - Where a rule of law requires that certain documents, records or information be retained that requirement is satisfied by retaining them in the form of electronic records. (See conditions in Article 9). - In the context of the formation of contracts, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic records. Where an electronic record is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that an electronic record was used for that purpose. Acknowledgement of receipt, time & place are regulated. - The portion of an electronic record that is signed with a digital signature shall be treated as a secure electronic record if the digital signature is a secure electronic signature in accordance to the Act.. - Persons relying on a digital signature will also rely on a valid certificate containing the public key by which the digital signature can be verified. - Duties of CAs and subscribers are enumerated in the Act. - The Minister shall appoint a Controller of Certification Authorities and shall The Minister may make regulation for operating and licensing of certification authorities and to define when a digital signature qualifies as a secure electronic signature. - Foreign certification authorities can be recognized.

	- The Act regulates the Government use of electronic records and signatures. Electronic Transaction (Certification Authority) Regulation in 1999: - It regulates the licenses (e.g. revocation, suspension) and licensing certification authorities. - It also states the rules for application to Government and statutory corporations.
Republic of Korea	- This year the Government passed the Basic Act on E-commerce, a privacy protection e-commerce act and an electronic signature act (a summary of the legislation can be found at the Baker & McKenzie website). - South Korea has two basic e-commerce laws: an umbrella law that broadly defines the concept of e-commerce, requirements of electronic documents and ecommerce dispute resolution; and an electronic signature law that stipulates the legal effects and certification requirements of digital signatures. Both laws were enacted in February 1999 and put in place on July 1st 1999. These laws are far from complete in their coverage, and they lack clear definitions of legal jurisdiction among government agencies over many different aspects of e-commerce. Still, they serve their purpose of providing the basic framework for local e-commerce. - The draft Bill on Promotion of Trade Business Automation contains a provision (article 14), which states that digital signatures of electronic documents for application or for approval shall be regarded as properly signed as stipulated by the laws and decrees relative to trade. - Public or private organisations meeting certain eligibility requirements may become official certification agencies to endorse 'signed' electronic contracts. Approval by the MIC is required for official certification agencies. - There are neither import restrictions nor prohibitions against using cryptography in the private sector. - The Republic of Korea restricts the export of cryptographic hardware and software pursuant to the Wassenaar Arrangement. Regulations on exports are governed by the Public Notice on Export and Import of Strategic Goods issued pursuant to the Foreign Trade Act and its accompanying Decree. The licensing authority for exports is the Ministry of Commerce, Industry, and Energy.
Sri Lanka	- As e-business is in still in infancy in Sri Lanka, there are no regulations dealing specifically with e-commerce. Relevant laws and regulations dealing with traditional trade are deemed to cover e-commerce. - Currently, no e-contract laws exist. Contracts entered into via the Internet are protected in the same manner as non-electronic contracts. Existing laws governing traditional commerce are deemed to cover e-contracts - Sri Lanka maintains no import, export, or domestic use prohibitions on cryptography. - Sri Lanka considers that CAs shall be established at national and international levels. - There are no significant initiatives regarding the establishment of CAs.
Thailand	- The Electronic Transaction Bill and Electronic Signature Bill have been approved on 14 March 2000 as part of the National IT Laws Project. - For Thailand, CAs shall be established at national and international levels.
Vietnam	- Vietnam does not yet have a coherent legal framework regarding e-commerce.

African Region

Country	Project of Law and/or Law briefing
Burkina-Faso	- CAs has no structured programme.
Ghana	Participant's information: - Ghana's legal framework is under review, - Parties to a contract can agree to use a different media than a written document to pass a contract and it is considered acceptable. (e.g. EDI contracts and other e-commerce services.). - There are no restrictions for import and/or export of encryption technologies and no domestic controls on the use of encryption technology for civilian use. - Strong encryption types are in use. 128-bit encryption is in use for financial applications. - The Government is encouraging e-commerce expansion and plan to use encryption technologies. Rather, The Government expressed concern on the earlier USA export restrictions of strong encryption based product to Ghana. - Electronic data, message, information and other can be presented as evidence at a Court, if appropriately supported with additional evidence such as logs etc. - There is no legislation on CAs and RAs. Private companies can and shall operate as CAs and/or RAs. CAs should be established at a national level in each country. CAs and RAs have to be authorized by the Authorities to provide certification, verification and registration services.
Kenya	- There is no law in Kenya governing digital signatures and electronic contracts. - Encryption technology can be imported into the country. - There is no government requirement for the keys to be stored by a government agency - There is no restriction on the encryption key size - Kenya is not a signatory to any agreements on encryption technologies - There is no clear government policy on the use of encryption technology - On September 16, 1998, the United States authorized the export of unlimited strength encryption products (with or without key recovery) to the banking and financial, insurance, health and medical, and on-line electronic commercial sectors in Kenya. This is an indication that the U.S. has leveraged its authority to gain access to plain text information in those sectors within the country under Mutual Legal Assistance Treaty (MLAT)/Financial Action Task Force (FATF) provisions.
Mauritius	THE ELECTRONIC TRANSACTIONS ACT. Published in the Government Gazette of Mauritius No. 79 of 11 August 2000 (Act No 23 of 2000): To provide for an appropriate legal framework to facilitate electronic transactions and communications by regulating electronic records and electronic signatures and the security thereof: - No record or signature shall be denied legal effect, validity or enforceability solely on the ground that it is in electronic form.

	- Where an enactment requires any information or record to be in writing, an electronic record shall satisfy that requirement where the information contained therein is accessible so as to be usable for subsequent reference. - Where an enactment requires that records, documents or information be kept, that requirement shall be satisfied where the records, documents or information are kept in the form of an electronic record in accordance with article 7. - Where any enactment requires a signature, or provides for certain consequences if a document is not signed, an electronic signature shall satisfy that requirement. - No contract shall be denied legal effect, validity or enforceability solely on the ground that an electronic record was used in its formation. No declaration of intent or other similar statement between the originator and the addressee of an electronic record shall be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record. - Where a prescribed security procedure, or a commercially reasonable security procedure agreed to by the parties involved, has been properly applied to an electronic record to verify that the electronic record has not been altered since a specified point in time, the record shall be treated as a secure electronic record from such specified point in time to the time of verification. - Any person relying on a digital signature shall also rely on a valid certificate containing the public key by which the digital signature can be verified. - CAs and certificates (issuance, suspension, revocation, etc.) are regulated by the Act. (See article 24 to 32). The public office of Controller of Certification Authorities will regulate the CAs activity. <u>Participant's information</u>: - Digital signatures are legally recognized by the Mauritius Law as per the Electronic Transaction Act 2000. Visit http://ncb.intnet.mu/mitt.htm for viewing the Act. - Electronic documents can be used to establish a contract or to sign a document in conformity with the Law. - There are no restrictions for import and/or export of encryption technologies nor domestic controls on the use of encryption technology for civilian use. There is no limitation on the encryption key size authorized for civilian use. - Electronic data, message, information and other can be presented as evidence at a Court. - Private companies can operate as CAs and/or RAs. CAs should not necessarily be established at a national level in each country. CAs and RAs have to be authorized by the Authorities to provide certification, verification and registration services.
Nigeria	- There is no specific legislation relating to e-commerce concerning contract law and dispute resolution in Nigeria.
South Africa	- Most of the country's existing laws are made without reference to e-commerce. Even though it is feasible that legislation concerning 'paper-based' transactions could apply to e-commerce, the problem lies in definitions. Words such as 'document', 'signature', 'writing', 'original', 'notice', 'record' and 'delivery' are difficult to apply in many cases to e-commerce transactions. - The current legal framework is tailored for paper-based commercial transactions. Laws contain provisions and terms ordinarily associated with paper-based documents and actions. - There are no domestic controls on the use of encryption in South Africa. There are many companies in SA active in the development of crypto products.

	- According to the Commerce/NSA report, the South African government controls encryption exports and imports as a dual-use item on the General Armaments Control Schedule. Exports of encryption require an individual validated license. The control of encryption is under the jurisdiction of the South African Department of Defense Armaments Development and Protection Act, 1968, No. R. 888, published on May 13, 1994. - An individual validated license was previously required for the import of encryption software. A valid permit from the Armaments Control Division is required for the import or transportation of cryptographic equipment or software. This information is gleaned from State Department Johannesburg Cable 000951, June 23, 1995.
Tanzania	- There are reportedly no controls on the export, import, and domestic use of cryptography in Tanzania. - By 1999, there was a policy review on the legal treatment of contractual issues in e-commerce. - Digital signatures are being implemented by the National Bank of Commerce; however no serious problems involving legal actions have been encountered.
Uganda	- There are reportedly no controls on the export, import, or domestic use of cryptography in Uganda. - By 1999, no specific legislative or regulatory effort was undertaken to adapt national contract law to account for the new challenges posed by electronic transactions. - There is an industry self-regulation, with government intervention only in cases of major abuse or neglect. - Uganda considers that CAs shall be established at national and international levels. - By 1999, no significant initiatives were undertaken on the establishment of CAs.

Europe & CIS region

Country	Project of Law and/or Law briefing
Armenia	- Armenia does not currently have a policy on the use of cryptography.
Bulgaria	- The Bulgarian government as of May 4th 2000 had approved in principle the Electronic Document and Electronic Signature Bill. Passage by the National Assembly is expected shortly. It should go into effect around the beginning of 2001. - Amendments to the Code of Criminal Procedure are in the process of being drafted which would make it illegal to forge electronic signatures. - There are no domestic or import controls on the use of cryptography. - Bulgaria has acceded to the Wassenaar Arrangement and is presumably committed to restricting the export of cryptographic-enabled software as a dual-use good. Bulgaria agreed to the enhanced Wassenaar controls announced in December 1998.
Croatia	- There are no domestic use, import or export controls for encryption in Croatia.
Cyprus	- There are no domestic use controls, export controls or import controls on cryptographic products in Cyprus. In addition, no government agency has established authority over cryptographic policy.
Czech Republic	- No separate legislation currently exists for e-commerce (it is guided only by the commercial code, just as any other retailer is). The government is working on a legal framework for the sector but it is not clear as to when any legislation aimed directly at e-commerce will be ready. However, most analysts expect it will broadly be in line with EU regulations. - In June 2000, parliament has adopted digital signature legislation. It came into effect on 1 October 2000. The law changes existing civil, criminal, tax and administrative laws. - Courts are notoriously slow and expensive, and have little or no experience in dealing with e-commerce issues. - The importation of encryption products (although not the domestic use thereof) is regulated by the Ministry of Industry and Trade. - A license (either a general license, an "open" license, or an individual license) from the Ministry is required for the importation of encryption products into the Czech Republic: a. The general license applies to low-level encryption products, as identified in Regulation No. 44/1997 Coll: (1) Encryption products covered by the general license may be imported without an import license, subject to notification to the Ministry; and b. An individual or an open import license is required for higher level encryption products: (1) The individual license is intended for single transactions and (2) The open license is intended to permit multiple imports (for example, by a distributor) over a one year period of time. - There are no corresponding licensing or approval requirements for the domestic distribution or use of encryption products, although users of imported encryption products may use those products only in accordance with the terms and conditions of the import license under which they were imported. - Importation of encryption products without the requisite import license from the Ministry is subject to fines of CZK 20 million (about US $556,000) or five times the value of the imported products, whichever is greater.
Hungary	- There are no rules in Hungary currently allowing electronic signatures of contracts. However, draft legislation on this topic is under preparation.

	The draft would implement EU guidelines. - A basic principle would be to make electronic signatures legally admissible and binding for those that choose to use them but ensure that no parties are ever forced to use them. - The new law would create objective standards for determining the legality of electronic signatures, which would be valid only in freely entered business transactions (not in state administration). The Law is fully in compliance in the EU principles. There will be two types: a simple electronic signature and a qualified electronic signature. - The draft law would seek to ensure that several conditions be present for an electronic contract to be valid: the identity of the signatories and the fact of signature must be 'establishable', for example. The time of signature will also be significant. There must also be conclusive evidence that the contract was not altered after signature. - The state will not introduce a licensing procedure for providers of electronic signature technology or services, according to the draft. - Binding agreements may be reached today in e-commerce in Hungary. - The courts determine the validity of electronic contracts and the origin of electronic documents on a case-by-case basis, with no clear guidelines. - There are no domestic controls on the use of cryptography in Hungary. - Hungary has implemented export controls on dual-use cryptography as required by the Wassenaar Arrangement, to which it is a party. In December 1998, Hungary subscribed to the more restrictive Wassenaar Dual-Use Control List. The Ministry of Economic Affairs licenses exports of encryption products. Import controls on cryptography also require a license in much the same manner as that applied to exports. - There are government guidelines and general oversight of private CA's. - Hungary considers that CA's shall be established at national and international levels. - By 1999, there were no significant initiatives in the establishment of CAs.
Kyrgyzstan	- There are no export, import, or domestic use controls on cryptography in Kyrgyzstan.
Malta	- On 18 May 2000 the Maltese Government launched a White Paper on the Legislative Framework for Information Practices. This White Paper includes three bills: the first one on Electronic Commerce, the second one on Data Protection and a third one dealing with computer misuse. - There are government guidelines and general oversight of private CA's. - Malta considers that CA's shall be established at national and international levels. - Some informal industry-based private authorities, under government guidelines have been established as CAs.
Romania	- There are no import or domestic use controls on cryptography in Romania. - Romania regulates the export of encryption pursuant to its participation in the Wassenaar Arrangement. The licensing authority is the Department of Foreign Trade of the Ministry of Commerce.
Russia	- The major e-commerce operators could create a specific organisation responsible for drafting the rules regarding electronic signatures and then supervise the activities of its association members. Such precedents exist in Russia--for example, MICEX, the equities/currency market--and can be directly applied to e-commerce.

	- The technological issues may be getting ahead of the broader legal framework, however, since electronic transactions and signatures currently have no equivalence under the law with paper-based transactions and signatures. Courts simply do not recognise claims based on electronic signatures. - The importation and distribution of encryption products is subject to regulation both by the Ministry of Trade and the Federal Agency for Government Communications and Information ("FASPI") under Russian Federal Law No. 158-FZ, dated September 25, 1998 and Presidential Decree No. 334, dated April, 1995 - Each importation of encryption products requires an import license from the Ministry of Trade: a. As a condition of issuance of that import license, the encryption product must first be approved by FAPSI, and b. The FAPSI approval process takes 1-2 months, and, approvals for foreign encryption products are not frequently granted except where the encryption products will be used by local subsidiaries of foreign corporations - The prior approval of FAPSI is also required for the distribution of encryption products (foreign or domestic) in Russia: a. The FAPSI approval for the importation of such encryption products does not constitute authorization to distribute those products to third parties within Russia, so a separate FAPSI distribution approval is required, and b. Such FAPSI approvals for the distribution of encryption products within Russia are also not frequently granted - Importation and/or distribution of encryption products without the requisite FAPSI approvals and Ministry of Trade import licenses (if applicable) are subject to fines and, in the case of individuals, including corporate officers, imprisonment for up to 5 years. - Russia is a participant in the Wassenaar Arrangement and restricts the export of cryptographic hardware and software. It adheres to the Wassenaar Dual-Use Control List announced in December 1998. The State Duma is poised to adopt a draft Federal Law on Electronic Digital Signatures that regulates the usage and verification of electronic digital signatures: - The Draft Law defines an electronic digital signature as a cryptographic symbol that requires a key to decode it. Approach is to state that only electronic digital signatures involving the use of public-key cryptography technology satisfy legal signature requirements. - The Draft Law also requires that the Russian government license all-certifying centres reviewing electronic digital signatures. -
Slovakia	- A new legislation has been drafted to adapt national contract law to account for the new challenges posed by electronic transactions. - The government has established and operates CAs. - For Slovakia CAs shall be established at national and international levels. - Concerning CAs existing industry-based private authorities, under government guidelines are run in Slovakia, - There are no domestic use controls of cryptography in Slovakia. - Slovakia regulates the export of cryptography pursuant to its participation in the Wassenaar Agreement. Slovakia adhered to the revised Wassenaar Dual-Use Control List announced in December 1998. The licensing authority is the Ministry of Economy. - Slovakia also regulates the import of cryptography. Import licenses are issued by the Ministry of Economy. Ref: http://www.wassenaar.org

	http://cwis.kub.nl/~frw/people/koops/cls2.htm
Slovenia	- There are no export, import, or domestic use prohibitions on cryptography. Significantly, Slovenia, unlike neighboring Croatia, was not on the list of countries eligible to receive U.S. general purpose encryption commodities and software under a U.S. Commerce Department license exception. This indicates that there are mutual legal assistance difficulties between the U.S. and Slovenia. Ref: http://cwis.kub.nl/~frw/people/koops/cls2.htm The Republic of Slovenia has adopted an Electronic Commerce and Electronic Signature Act. The law came into effect on 22 August 2000: - This act regulates electronic commerce, which includes commerce in the electronic form on distance by the use of information and communication technology and use of electronic signature in legal affairs, including electronic commerce in judicial, administrative and other similar procedures. - Legal effectiveness and admissibility as evidence shall not be denied to the data in the electronic form solely on the grounds that they are in the electronic form. - The Act regulates the acknowledgement of the reception of e-messages. - Where the law or any other provision requires that certain documents, records or data be retained, that requirement is met by retaining electronic data, if some requirements are met (See Article 12). - Where the law or any other regulation requires information to be in writing, that requirement is met by an electronic message, if the information contained therein is accessible so as to be usable for subsequent reference. Some type of contracts are excluded from this provision. (See Article 13). - Electronic signature shall not be denied legal effectiveness or admissibility as evidence solely on the grounds of its electronic form or not being based on a qualified certificate or a certificate issued by an accredited certification service provider or not being created by a secure signature creation device. - Advanced electronic signature, verified with qualified certificate, is equal to autographic signature in relation to data in electronic form, and has therefore equal legal effectiveness and admissibility as evidence. - Certification service provider does not require a special permit for performing his activity. - The Act contains provisions regulating the Certification Service Providers (CSP), the certificate holder, certificates, technical requirements for secure signature creation, etc. - Ministry performs the supervision over the implementation of the provisions of this act. - An inspector can control the CSP. The Agency for telecommunications will be the accreditation body that shall perform the supervision and the official actions over the accredited certification service providers. - Qualified certificates of the certification service provider with a place of business originating from European Union are equal to domestic qualified certificates. Those with origin on the third countries are equal to domestic qualified certificates, after fulfillment of some requirements. (See Article 46).
Turkey	- Turk Telekom only began testing ATM technology in 1998, with X.25 and frame relay remaining the main data transportation solutions.

	- No specific legal provisions currently govern digital signatures. In general, traditional contractual agreements are secure in Turkey. Where differences arise, foreign companies have the same legal right of recourse to the courts as their Turkish counterparts. - There are no import or domestic controls on cryptography in Turkey. - Turkey restricts the export of cryptography pursuant to its participation in the Wassenaar Arrangement. Exports must be registered in accordance with Article 3a of the Export Regime Decree No. 95/7623 of December 22, 1995. The governing authority is the Under-secretariat for Foreign Trade (UFT). Cryptographic products for export must be registered with the Istanbul Metals and Minerals Exporters' Association (IMMIB), which assigns a registration on the applicable customs declaration. Law No. 3763 of 1940 regarding the "Control of Private Industrial Enterprises Producing War Weapons, Vehicles, Equipment, and Ammunition" requires a permit from the Ministry of National Defense for the export of cryptographic products having military purposes. The export laws only apply to tangible software. - By 1999, no specific legislative or regulatory effort was undertaken to adapt national contract law to account for the new challenges posed by electronic transactions. - There are some government guidelines and general oversight of private CAs - For Turkey CAs shall be established at national and international levels. - By 1999, there were no significant initiatives on the establishment of CAs
Ukraine	- There are no specific laws prohibiting the import or use of encryption in the Ukraine. Ukraine regulates the export of cryptography pursuant to its participation in the Wassenaar Agreement. Ukraine adheres to the revised Wassenaar Dual-Use Control List announced in December 1998. The export licensing authority in Ukraine is the State Export Control Service.

Arab States Region

Country	Project of Law and/or Law briefing
Egypt	Participant' s information: - There is a final report on a draft project concerning e-commerce to be discussed in the Information Technology Committee of the majority party. This is a step towards submitting the draft law to the Parliament during its present session. - The draft law aims at the security of the transaction, which take place through the electronic media. - It also aims to provide equal legal validity to the electronic documents and signatures as it is given to paper documents and handwritten signatures. - The draft law shall provide for equality of written usual contract with electronic contracts as long as it fulfills the terms and conditions. - The Central Bank shall set the rules for certifying the electronic signature and to give license permits for practicing certification of electronic signature according to established terms and conditions. - The principle of cryptography of data according to specific rules and regulations for encrypting the electronic documents and data is accepted. An encryption office shall be established for depositing the encryption keys, safeguarding the encrypted data, which cannot be decoded unless according to a court decision. - The draft provides for the terms and conditions to validate the electronic documents ad signatures in front of the courts.
Jordan	General Principles: - The government should avoid imposing unnecessary regulations or restrictions on electronic commerce. - The private sector should lead in the development of electronic commerce and in establishing business practices. - Electronic commerce will help the government to serve its people better, by increasing efficiency of public services and products. - The government should work towards a global approach that supports, domestically and internationally, the recognition and enforcement of electronic transactions and electronic authentication methods (including electronic signatures). At an international level this should include working together on a convention or other arrangements to achieve a common legal approach that will support electronic transactions as well as a variety of authentication technologies and implementation models. This approach should: a. Remove paper-based obstacles to electronic transactions by adopting relevant provisions from the UNCITRAL Model Law on Electronic Commerce; b. Permit parties to a transaction to determine the appropriate authentication technologies and implementation models for their transaction, with assurance that those technologies and implementation models will be recognized and enforced; c. Permit parties to a transaction to have the opportunity to prove in court that their authentication technique and their transaction is valid; d. Take a non-discriminatory approach to electronic signatures and authentication methods from other countries.
Morocco	- There are reportedly no domestic use controls, export, or import controls on cryptography in Morocco.
Saudi Arabia	- The Ministry of Commerce in January 2000 established a permanent technical committee to prepare a legal framework for online trade. - It is reported that Saudi Arabia prohibits the domestic use of encryption. According to the NIST survey, Saudi Arabia has neither import nor export

	controls on cryptography in effect. - Companies and private persons can use technology upon authorization.
Syria	- In 1999, no specific legislative or regulatory effort was undertaken to adapt national contract law to account for the new challenges posed by electronic transactions. - Concerning the CAs there is an industry self-regulation, with government intervention only in cases of major abuse or neglect - Syria considers that CAs shall be established at national and international levels. - Some informal industry standards, loosely defined under the law have become CAs in Syria.
Tunisia	- According to Decree No. 97-501 of March 14, 1997, Tunisian value-added telecommunications service providers must first obtain authorization to encrypt communications. Encryption keys must be deposited with the government. The Ministry of Communications may, in certain cases and in the interests of national security and public safety, partially or totally revoke authorizations granted to value-added telecommunications services to encrypt communications.
United Arab Emirates	- There are reportedly no export, import, or domestic use prohibitions on cryptography. - By 1999, there was a policy review on the legal treatment of contractual issues in e-commerce underway - The Government established and operates CAs. - The United Arab Emirates (U.A.E.) considers that CAs shall be established by national authorities. - Existing industry-based private authorities, under government guidelines are operating in the U.A.E.

Bibliography

⇒ ***Asociación Latinoamericana de Integración (ALADI)***, *"Situación Actual y Perspectivas del Comercio Electrónico en los Países Miembros de la ALADI". Versión Preliminar. Segunda Parte. Restringido. ANEXO VI. Disposiciones de los países miembros de la Asociación sobre comercio electrónico.* ALADI/SEC/di 1347. 19 July 2000, 136p.

⇒ **Baker & Mc Kenzie** web site. http://www.bmck.com/ecommerce/ Visited between July – November 2000

⇒ **Baker & Mc Kenzie *Abogados*, S.C.** web site. One e-commerce world. One firm. Connected. Clients Bulletin / E-Commerce Amendments. Mexico. May 2000. www.bakerinfo.com/ecommerce

⇒ ***Comisión redactora del Anteproyecto de Ley de Firma Digital para la República Argentina***. Buenos Aires, 18 August 1999. http://www.business-net.com.ar/notas_de_secciones/legislacion/AnteproyectodeLeydeFirmaDigitalparalaRepublicaArgentina.htm Visited on 23rd January 2001.

⇒ **Digital Signature Law Survey**, by Simone van der Hof. http://rechten.kub.nl/simone/ds-lawsu.htm Visited on 23rd January 2001.

⇒ **Electronic Privacy Information Center**. Cryptography and Liberty 1999. An International Survey of Encryption Policy. Washington, DC Visited between July – November 2000 http://www2.epic.org/reports/crypto1999.html

⇒ ***El Panamá América* journal**. *Finanzas*. Article: *Senacyt presentará anteproyecto de ley sobre comercio electrónico en Panamá.* Sunday, 2 July 2000, *Editora Panamá América, S.A. (EPASA)* http://www.epasa.com/El_Panama_America/archive/07022000/finanzas.html

⇒ **International Telecommunication Union**, Report on the e-commerce survey conducted in the framework of World Telecommunication Day 1999. Policy Considerations for Electronic Commerce: ITU Member Views. http://www.itu.int/newsarchive/wtd/1999/report_toc.html Visited in November 2000.

⇒ **International Trade Centre UNCTAD/WTO**, Secrets of Electronic Commerce, A guide for Small-and Medium-Sized Exporters, An ITC Technical Publication for Developing Countries, Trade Secret Series, Questions, Answers & Reference Guides. 07.04 SEC, Abstract 2000, 215 p. Doc No. ITC/290/1B/00-VII-TP.

⇒ ***La Firma* Digital.com,** Derecho y Nuevas Tecnologías, Copyright 2000. Visited on December 2000. http://www.lafirmadigital.com/

⇒ **McBride Baker & Coles International Database for E-Commerce and Digital Signatures.** Visited on 24th January 2001.

http://www.mcbridebakercoles.com/ecommerce/international.asp

⇒ **Nishith Desai Associates.** Draft Copy. International Conference on Electronic Commerce organised by Infrastructure Leasing & Financial Services Limited Global Information Infrastructure Commission and Confederation of Indian Industry Legal and Policy Framework for E-Commerce in India. Private & Confidential. http://www.giic.org/pubs/indiawhitepaper.pdf

⇒ **Participant countries reply to the ITU/EC-DC Survey on the e-transaction, digital signature, CAs, and RAs legal environment**. Dated December 2000.

⇒ **The economics web site, ebusinessforum.com Global Business Intelligence for the Digital Age.** http://www.ebusinessforum.com/index.asp?layout=channelid_6&channelid=6&title=Doing+e-business+in Visited between July – November 2000.

⇒ **Venezuelan American Chamber (Venamcham) and Cavecom.** *Borrador del Proyecto de Ley Conjunta entre Venamcham y Cavecom. Ley de Reconocimiento Legal de Mensajes de Datos y Firmas Electrónicas.* 11/12/a. October 2000.