



The African Region (including Arab countries)

Legal framework for e-commerce

Last updated: 3 Sept. 2002

	Country	Project of Law and/or Law briefing
1	Burkina-Faso	<ul style="list-style-type: none"> - Since June 2002, the government of Burkina Faso is working on a new legal framework applicable to electronic commerce, certification authorities, registration authorities, digital signatures, data protection, privacy protection, consumer protection, cyber crime, liability of intermediaries, copyrights, etc.
2	Cap Vert	<ul style="list-style-type: none"> - The <i>Documentos e actos juridicos electronicos</i> from 13 November 2000 is inspired in the Portuguese legislation. It establishes the legal framework that validates and provides legal effects to electronic contracts and digital signatures and any other e-signature that satisfies similar security requirements to those applicable to digital signatures. - The Act stipulates that e-documents can be presented as evidence to a Court. The current law regulates the sending and reception of e-documents and mentions that the operations through which the transfer of such documents is done cannot read its content, or duplicate it, or distribute it to third parties (exception). - Public organs can issue e-documents digitally signed. - Digital signatures annexed to a document replace, for any legal effects, the seals, brands, and other signal that identifies its owner. - The abovementioned legislation regulates certification, digital certificates, certification authorities, accreditation authority,
3	Egypt	<p>Participant' s information and www.arabicnews.com info:</p> <ul style="list-style-type: none"> - 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. The new law would help national banks introduce new e-technology and services for their clients and will provide security and regulations for banks. - 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 Law will recognize e-signatures and help to protect e-commerce transactions in banks from hackers and set new legal penalties against forgers of e-signatures. - The draft provides for the terms and conditions to validate the electronic documents ad signatures in front of the courts - The draft law shall provide for equality of written usual contract with electronic contracts as long as it fulfills the terms and conditions.

		<ul style="list-style-type: none"> - 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.
4	Ghana	<p><u>Participant's information:</u></p> <ul style="list-style-type: none"> - 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 et. - 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.
5	Kenya	<ul style="list-style-type: none"> - 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.
6	Mauritius	<p><u>THE ELECTRONIC TRANSACTIONS ACT</u>. 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</p>

		<p>electronic records and electronic signatures and the security thereof:</p> <ul style="list-style-type: none"> - 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. <p><u>Participant's information:</u></p> <ul style="list-style-type: none"> - Digital signatures are legally recognized by the Mauritius 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.
7	Morocco	<ul style="list-style-type: none"> - There are reportedly no domestic use controls, export, or import controls on cryptography in Morocco. - <i>Les lois actuellement en vigueur pour la conclusion et l'exécution de contrats sont adéquates, excepte pour le commerce électronique. Le pays possède un nouveau système de cours de commerce et offre une formation sur la loi commerciale aux juges, mais les actions en justice relatives à ce domaine ne sont pas traitées de façon</i>

		<p><i>diligente par le système judiciaire.</i></p> <ul style="list-style-type: none"> - <i>La loi actuellement en vigueur ne reconnaît pas la signature électronique. Le gouvernement doit procéder à une réforme de ces lois dans le but de reconnaître légalement les signatures et le paiement électroniques.</i> - <i>Le Maroc a assigné à l'agence ANRT la mission d'élaborer les lois de cryptage conformément aux paramètres acceptés à l'échelle internationale.</i> - <i>Le Maroc a besoin de reconsidérer la protection offerte à la propriété intellectuelle et de l'adapter aux standards internationaux car la loi actuelle sur la protection des droits d'auteur ne fournit pas assez de protection et ne traite pas la protection des logiciels.</i> - <i>Le Secrétaire d'Etat chargé des Postes et des Technologies de l'Information prévoit de présenter au gouvernement des projets de loi régissant le commerce électronique (en 2002)</i> <p>Source : http://usembassy.morocco.org.ma/</p>
8	Nigeria	<ul style="list-style-type: none"> - There is no specific legislation relating to e-commerce concerning contract law and dispute resolution in Nigeria.
9	South Africa	<ul style="list-style-type: none"> - 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. - South Africa has new legislation on e-communications and transactions act since August 2002. The legislation removes many existing barriers to e-commerce. The government is now obliged to develop a national e-strategy consisting of an action plan to stimulate and promote the use of Internet and e-commerce. - The bill is essentially divided into the following parts: legal requirements for data messages, communication of data messages, registration of cryptography providers, authentication providers, consumer protection, protection of personal information, protection of databases, e-government, domain names authority, cyber inspectors, and cyber crime. - E-mails, Internet and other e-messages are given legal status; all documents and

		<p>agreements that had to be, by statute, in writing, signed, retained in an original format may now be in e-format; legal agreements may be concluded online and electronically; agreements concluded with e-agents, such as websites, are given legal effects; there shall be a cooling off period for good and services purchased over the Net for the consumer to cancel the transaction; spamming shall be illegal (with exceptions); hacking, computers related extortions and forgery are made crime.</p> <ul style="list-style-type: none"> - The law also establishes the requirements that businesses must fulfill in order to collect data from consumers. - The sending and reception of a messages are regulated by the law. <p>Source: http://www.hq.org/art246.html Hieros Gamos.</p>
10	Tanzania	<ul style="list-style-type: none"> - 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.
11	Tunisia	<ul style="list-style-type: none"> - 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. - The country has an electronic exchanges and electronic commerce bill since August 2000. E-contracts are governed by written contracts procedures concerning the expression of will, its legal power, its validity, its execution liability, as long as they are not in contradiction with the bill. The bill regulates e-documents, e-signatures, certification authorities, e-certification services, e-commerce transactions, privacy protection, and infractions and penalties. Source: www.bakernet.com
12	Uganda	<ul style="list-style-type: none"> - 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.