fastforward

Trinidad and Tobago. Accelerating into the digital future.

"NATIONAL POLICY ON ELECTRONIC TRANSACTIONS"

December 2005

Table of Contents

1.0 INTRODUCTION 1

2.0 BACKGROUND 2

2.1 Why is an Electronic Transactions Policy Necessary? 2

2.2 What are Electronic Transactions and e-Commerce? 3

2.4 Linkages with Other Laws 4

2.5 Legislative Approach 4

2.6 The Electronic Transactions Bill 5

2.7 New Initiatives under the Electronic Transactions Policy 6

3.0 OBJECTIVES OF THE ELECTRONIC TRANSACTIONS POLICY 8

4.0 PRINCIPLES 11

4.1.1 Definitions 11
4.1.2 Binding the State 12
4.1.3 Exclusions 12
4.1.4 Voluntary use of electronic transactions 13
4.1.5 Consent may be inferred 13
4.1.6 Express consent required for government 13
4.1.7 Certain legal requirements continue 13

4.2 Principle 2: Requirements for Legal Recognition 13

4.3 Principle 3: Contract Formation and Default Provisions 14
4.3.1 Formation and validity of contracts 14

4.4 Principle 4: Electronic Signatures 15

4.5 Principle 5: Certification Service Providers 16
4.5.2. Registry of certification service providers 16
4.5.10 Recognition of external certification service providers 17
4.5.11 Pseudonyms 17
4.5.12 Additional responsibilities of a certification service provider 17
4.5.13 Immediate revocation upon request 18
4.5.18 Costs of an audit 18

4.6 Principle 6: Intermediaries and Internet Service Providers 18

4.7 Principle 7: Government and Other Public Bodies 19
4.7.1 General authorisation 19

4.8 Principle 8: Consumer Protection 19
4.8.1 Minimum information in e-commerce 19
4.8.3 Unwanted commercial communications (“spam”) 20

5.0 REFERENCES AND BIBLIOGRAPHY 22

1.0 Introduction

The Ministry of Public Administration and Information (MPAI), through extensive consultation with the public sector, the private sector and academia, developed ***fastforward***, the National Information and Communications Technology (ICT) Strategy for Trinidad and Tobago. ***fastforward*** is a comprehensive plan to leverage the power of people, innovation, education, information technology and infrastructure to accelerate social, economic and cultural development for all elements of society.

Electronic commerce ("e-commerce") is at the heart of the information economy and the Government of Trinidad and Tobago intends to promote the increased use of e-commerce as a catalyst for economic growth within the global marketplace. Substantial legal and policy change is anticipated as part of Trinidad and Tobago's evolution toward a knowledge-based economy. For e-commerce to flourish in Trinidad and Tobago, we must have a clear and predictable legal environment that can be trusted by citizens, institutions and businesses. Two key areas in which legislation is required are Data Protection and Electronic Transactions. This document develops the Electronic Transactions Policy, which forms the basis of the Electronic Transactions Bill.

The Government is responsible for providing the legal stability that allows for certainty and mitigates the risks of transacting electronically both locally and internationally. Citizens must be provided with the same protections that they have when conducting business face-to-face and using paper documents. Business must be able to make and enforce e-contracts and have the confidence to invest in new technologies and take advantage of new opportunities. The approach taken to provide legal certainty must be compatible with internationally accepted best practices so that business and consumers can freely operate across international borders. The Electronic Transactions Bill is *enabling* legislation that facilitates the use of modern communication technology and promotes the growth of electronic commerce.

This document sets out the policy that guides The Electronic Transactions Bill. The Bill draws upon a variety of sources, including the United Nations Commission on Trade and International Law (UNCITRAL) Model Law on Electronic Commerce, the UNCITRAL Model Law on Electronic Signatures, the European Parliament and Council Directive for a Common Framework for Electronic Signatures, and the legislation of other jurisdictions, including Singapore, Bermuda, New Zealand, Australia, Saint Vincent and the Grenadines, Sweden, Denmark, Norway and several Canadian provinces.

The central purpose of the Electronic Transactions Bill is to enable the objectives of ***fastforward*** to be achieved by enhancing trust in electronic commerce, removing barriers to the use of electronic transactions, clarifying the legal status of electronic documents, providing default rules governing electronic contracts, establishing a structure to recognise electronic signatures, and fostering good business practices by intermediaries and internet service providers. As a consequence, Trinidad and Tobago will have the tools to partake and progress in the
global information economy.

2.0 Background

2.1 Why is an Electronic Transactions Policy Necessary?

For developing countries, e-commerce has the potential to accelerate business development through increased efficiency and reduced costs in business operations. It provides new business opportunities by facilitating access to foreign markets. It also allows business to participate in new activities, such as data and records processing, customer service and call centres, and software application development. In fact, numerous governments have announced that fostering e-commerce is a major public policy objective to achieve economic growth. Governments themselves are often in the forefront of the e-commerce revolution in developing countries by launching their own Web sites to better communicate with and serve citizens, while reducing transaction costs. As well as providing a model for technological "take up," governments find that e-government, by promoting transparency and accountability, strengthens democratic structures and civil society.

The main non-technology components for e-commerce success are economic in nature. The response of private industry to the strategy for e-commerce development and the growth of trading markets will determine how successful Trinidad and Tobago is at entering the electronic marketplace. Necessary support, however, has to come from public policy initiatives that create a stable legal and regulatory environment. Just as governments have long secured the infrastructure of market economies by providing courts to enforce contracts, a land registry system, a securities regulatory structure and the like, similarly in the information society, governments have recognized the need to establish the infrastructure necessary to underpin e-commerce. Currently, there is uncertainty about the legal recognition of electronic documents, thus raising questions about the enforceability of electronic contracts or the use of electronic documents in litigation and enforcement proceedings. A number of statutes or regulations use terms, such as "document" or "copy" or "filing," that imply the use of a paper document. Other legislation requires signatures, witnessed signatures, or seals, all of which also imply a paper-based environment. These requirements are particularly common in regulatory statutes and are a barrier to the introduction of e-government and on-line government services.

To foster trust in e-commerce, consumers must know that contracts they enter into with suppliers of goods or services on-line have the same basic legal protections as contracts made face-to-face. To aid consumers in dealing with on-line suppliers, the Government is developing a Model Code for Consumer Protection in e-Commerce. The Code will educate consumers and business about what constitutes good business practice in an electronic business environment. In addition, the Electronic Transactions Bill sets out requirements for minimum information that businesses in Trinidad and Tobago must provide consumers when contracting electronically. These include information about the place of business and how to contact the business directly by mail or phone.

Greater certainty is also required as to the validity and reliability of electronic signatures. Furthermore, w hile general contract law has adapted to electronic communications, the nature of modern cyber-commerce creates uncertainties about such matters as the time of sending and receipt of the communication when the parties themselves have failed to set their own rules. To provide greater certainty, governments have been setting out guidelines and default rules for the conduct of e-business. Legislation that clarifies these issues encourages consumers in new markets to enter into business relationships since they know that the courts will have the necessary reference points to interpret contractual agreements. The Government itself will be able to more effectively implement its ***fastforward*** strategy for e-government since its authority to deal with the public electronically and to carry out its work in a more efficient manner is confirmed in the Electronic Transactions Bill.

Unwanted electronic communications or "spam" has moved beyond being an annoying or even offensive nuisance to individuals and businesses to being a serious problem that threatens broader interests. If spam is defined as "unsolicited commercial email," it accounted for as much as 80 percent of global email traffic in 2004. The very viability of the Internet as an effective means of communication is at stake, as is consumer confidence in electronic transactions and e-commerce. Spam can be a source of malicious

harm, interferes with legitimate commercial e-mailers, and causes serious productivity losses, as well as increasing costs for Internet service providers and other intermediaries. Ultimately, spam can significantly reduce the economic and social benefits expected from the growth of e-commerce. The Electronic Transactions Bill is part of a broader strategy that will include criminal sanctions, consumer education, codes of conduct, and active co-operation with business and other stakeholders to reduce the proliferation of unwanted communication.

2.2 What are Electronic Transactions and e-Commerce?

In a commercial and civil context, transactions (data messages and information) conducted over electronic networks are considered to be electronic transactions. These electronic means include, but are not limited to, e-mail and the Internet, electronic data interchange (EDI), telegram and facsimile. The term "transaction" should be interpreted broadly to include non-commercial transactions, single communications and the outcome of multiple communications (e.g., a contract). Transactions may be initiated by a human individual or by an electronic agent, that is, the term may include communications from machine to machine. E-Commerce is a particular type of electronic transaction and can be defined as the conduct of commercial activities by means of computer-based information and communications technologies. It generally involves the processing and transmission of digitized information. Examples of e-commerce range from the exchange of vast amounts of assets between financial institutions or the interchange of electronic data between wholesalers and retailers to telephone banking or the purchase of products and services on the Internet by consumers.

2.3 What are Electronic Signatures?

Signatures on documents perform a number of functions, such as identification, authentication, declaration of intent, authorization, safeguarding against undue haste, integrity and originality. E-commerce will not develop to its full potential until there is a sufficiently trusted means of communicating and authenticating communications—of performing functions similar to the written signature. The purpose of electronic signatures is to offer technical means by which the characteristics of signatures can be duplicated in electronic form.

Various forms of electronic signatures are possible and no doubt over time more will be developed. For this reason it is important not to lock in a particular technology in legislation dealing with electronic signatures. Currently, electronic signatures include biometric devices, use of personal information numbers (PINS), and digital signatures. These techniques provide different levels of security and are appropriate in different circumstances. Digital signatures are the most common of the more secure methods and are created and verified by a technique known as public key cryptography. Usually algorithmic functions are used to generate two different, but mathematically related, "keys." One key, known as the "private key," is used to create the signature and the other, the "public key," is used to verify the signature. The signatory must keep the private key secret since that is the basis for authenticity, although the signatory does not need to know the key but can use a smart card or other device to "sign." The public key cannot be used to re-create the private key so it is possible for many people, including public institutions, to have a copy of the public key.

Certification by a "trusted third party" is an important element of digital signatures. The relationship between the holder of the private key and its associated public key must be capable of authentication or verification. The public key must be accessible; if the parties know each other, this can be done by prior arrangement. To make full use of e-commerce, however, strangers must be able to establish trust. Certificate service providers can operate as trusted third parties to certify the identity of the parties exchanging information over the Internet. Certificate service providers can also perform other functions, such as notary or time-stamping services.

Government can play a role in ensuring that certificate service providers are reliable by providing the public with information about certification service providers that are registered and meet requirements that ensure their reliability and the integrity of their services.

2.4 Linkages with Other Laws

The intent of the Electronic Transactions Policy is to remove impediments to the conduct of electronic transactions that may be found in existing legislation and to ensure that no new barriers are created by new legislation or policies. There is a direct impact on legislation or legal practices in the following areas:

- Law of contracting and the commercial code;
- Evidence Act and admissibility and validity of electronic transactions;
- Exchequer and Audit Act;
- Computer Misuse Act;
- Freedom of Information Act;
- Intellectual property;
- Consumer protection;
- Laws that protect personal and corporate information.

2.5 Legislative Approach

Governments around the world have taken similar approaches to dealing with the issue of recognizing the validity of electronic documents. Generally speaking, all legislation dealing with electronic transactions or electronic documents states that no document, record or transaction will be found to be invalid solely because it is electronic in nature. The legislation creates **media neutrality**. It is important to note that a transaction may be invalid for other reasons—a contract that was entered into under duress will be no more valid if electronic than it were written on paper. A document that is irrelevant to a legal proceeding will be excluded as evidence by a court whether it is an electronic or paper document. The provisions regarding validity do not afford any greater evidentiary weight to electronic documents than to paper documents. The Bill does not give electronic documents any greater certainty than paper documents and basic contract law is not changed by electronic transactions legislation.

Governments have also adopted the basic concept of **functional equivalence** found in the UNCITRAL Model Law: where statutory language assumes the use of a paper document or paper-based transaction (e.g., by using a term such as "signature" or requiring the retention of records), the electronic transactions legislation will set out the criteria or tests that have to be met for electronic technology to fulfill the functions of the paper-based requirement. For example, one of the functions of providing individuals with paper copies of transactions is so they can review, re-read, and store them for future reference. If electronic technology allows for retention and storage for future reference and allows an electronic document to be printed, then it is said to be functionally equivalent. Also following the UNCITRAL Model Law, most electronic transactions legislation is **technologically neutral**. While it may set out criteria to determine functional equivalencies, it does not state what technology will satisfy the criteria since this may change over time.

The Electronic Transactions Bill is primarily enabling legislation that allows individuals and businesses to use electronic communications for personal and commercial purposes while knowing that their communications and transactions will have the same protections in court as paper documents. The Government will be able to effectively implement its e-government initiatives to provide better service to citizens and enhance transparency and accountability. In some areas, however, the Bill does create regulatory requirements dealing with such matters as the following: electronic signature providers and accredited signatures; improved protection for consumers doing business online; responsibilities of Internet service providers and other intermediaries; and limitations on unsolicited electronic communications or "spam." In these areas, the Government has generally chosen to take a "light touch" governance approach. For example, it establishes a regime where parties have considerable freedom to determine what form of electronic signature, if any, may be suitable for their purposes. The legislation, however, sets out criteria that define what may be considered a more secure or more reliable form of signature and creates a registration and regulatory regime to ensure the reliability and integrity of electronic signature service providers offering a more secure form of "accredited" electronic signature.

Government has chosen "**co-regulation**" as the form of "light touch" regulation in this Policy and the Electronic Transactions Bill. For example, the provisions of the Bill dealing with consumer protection in e-commerce emphasize codes of conduct, consumer education, and the role of industry organisations in fostering improved e-commerce business practices, including the limitation of "spam." Co-operation and sharing of responsibilities define this form of co-regulation. Both Government and business, as well as other stakeholders, must assume responsibilities under this approach. Business organisations will find that their new role to promote and monitor responsible business practices will improve industry reputations, while giving their members the freedom and flexibility to pursue the efficiencies and opportunities offered by e-commerce. Business, consumers and other stakeholders will have opportunities to be closely involved in defining good business practices and monitoring compliance with codes of conduct. Government and business will both have responsibilities in educating consumers and disseminating information about consumer rights and good practices. Government and industry organisations will also have a role in ensuring that small business receives the guidance it will need so that the new e-commerce environment does not introduce uncertainties and that the co-regulatory approach does not impose additional costs on small enterprises.

Government continues to play an active role under co-regulation by enforcing regulatory requirements through prosecutions and other sanctions and ensuring compliance with good business practices by monitoring and other administrative measures. The Government will also take action against anti-competitive conduct if it occurs. The Government believes, however, that co-regulation encourages the flexibility that is demanded in the rapidly changing electronic environment and to support business in Trinidad and Tobago in acquiring the maturity and capacities necessary for success in the global marketplace.

2.6 The Electronic Transactions Bill

This Electronic Transactions Bill will give legislative force to this Policy in the following ways:

- The Electronic Transactions Bill facilitates the use of electronic technology by providing that electronic methods of communication are legally effective and that legal requirements developed in a paper-based society may be met by using electronic technology that is functionally equivalent to those requirements.

- The Bill is based on three internationally accepted principles: media neutrality, technical neutrality and functional equivalence. *Media neutrality* means that electronic transactions and paper-based transactions should be treated the same by the law. *Technological neutrality* recognises the rapidly changing technological environment in which e-commerce and global communications operate. Legislation should not be based on particular technologies but should be structured in a manner that is independent of technological platforms so that innovation and technological experimentation are not compromised. *Functional equivalence* recognises that electronic transactions can be functionally equivalent to paper-based transactions and that there should be no discrimination between the two forms of transaction where the functional effect of a legal provision (e.g., that a document be "signed") can be met through equivalent electronic means.

- The Bill does not require that persons use, provide or accept information in electronic form without their consent. The Bill clarifies that contracts entered into electronically are valid and sets out certain "default" rules for such matters as time of dispatch or receipt of an electronic communication. It leaves a high degree of choice to parties to transactions to determine their own arrangements regarding the use of technology. It does not change the basic laws of contract.

- The Bill does, however, provide for some exclusions from the recognition of the legal effect of electronic documents and electronic signatures. In some cases, it is important to have only a single original of a document or it may be important to maintain the more formal or ceremonial aspects of the action of physically signing a document. The exclusions set out in the Bill are for wills, trusts

created by wills, powers of attorney, provisions requiring the production of original documents for immigration, passport or citizenship purposes, and provisions relating to dealings in land or real property. Additional exclusions may be created by order of the Minister.

- The Bill authorizes the use of electronic signatures since effective use of electronic communications often require the electronic equivalent of a signature, The Bill sets out criteria for an accredited form of electronic signature that meets requirements for reliability and authenticity; and establishes a "light touch" co-regulatory structure for recognizing trusted third parties or other certifiers of the authenticity of accredited electronic signatures.

- A major purpose of the Electronic Transactions Bill is to facilitate the introduction of e-government. Consequently, the proposed legislation ensures that the Government is able to transact business electronically, including receiving or making payments of money, maintaining records, collecting, storing, transferring, receiving or otherwise handling information and documents. So that Government will have an opportunity to introduce electronic services in an orderly manner, explicit consent of government ministries and other public bodies will be required before they transact business electronically.

- The Bill introduces protections for consumers who take advantage of the opportunities for choice offered by e-commerce by setting minimum requirements for information to be provided to consumers entering into electronic contracts, such as the place of business of the party offering goods or services to the consumer. It also requires a technical means of correcting input errors prior to placing an order, and addresses the enforceability of a contract made between a consumer and an electronic agent of the other party where the consumer has made a material error that he or she did not have an opportunity to correct.

- The Electronic Transactions Bill also forms part of the Government's strategy to deal with the rapidly developing problem of unsolicited electronic communications, often referred to as "spam." The Government will also be examining the need to update legislation to deal with "cyber-crime," including the use of spam to commit fraud. This Policy's companion Policy on Data Protection deals with spam that "harvests" personal data without the individual's consent. The Electronic Transactions Bill, however, deals with the sending of unsolicited commercial email and establishes rules for "opting out" of the receipt of unsolicited commercial messages. The spam provisions deal with emerging problems with unsolicited messages delivered by means of various electronic media, such as fax, voice mail and mobile phone. Consistent with the principles underlying the Bill, the provisions dealing with spam are both technologically and media neutral.

- The Telecommunications Authority of Trinidad and Tobago has the mandate to develop service standards and the code of conduct for intermediaries and Internet service providers. The standards and code will deal with such matters as knowing the customer, protecting personal data, procedures to deal with "spam," and developing an adequate system of settling customer disputes to encourage a competitive market of internet service providers and to promote good business practices.

- The Electronic Transactions Bill limits the liability of intermediaries and Internet service providers in certain circumstances; namely, where there is no actual knowledge that information may create civil or criminal liability and where legally authorized procedures to deal with illegal content are followed when required. Compliance with the prescribed standards and the code of conduct may also affect the availability of limited liability.

2.7 New Initiatives under the Electronic Transactions Policy

The Electronic Transactions Policy includes new procedures and processes designed to ensure that the objectives of the Policy and the Electronic Transactions Bill will continue to be met. It is now Government

policy to monitor global developments in e-commerce legislation and policy to ensure that the legislation and policy of Trinidad and Tobago remains compatible with and aligned to the developing international legal environment.

It is also now Government policy to review new policy initiatives, including the development of new legislation, to ensure that barriers to the use of electronic communication and e-commerce are not inadvertently introduced.

In addition, it is Government policy to establish a system of continuous consultation with the private sector and civil society to promote industry self-regulation or co-regulation, where appropriate, and to improve understanding of market demands. At the same time, Government will continue to provide broad-based policy guidance through education, the promotion of codes of conduct, and the fostering of self-regulatory and co-regulatory capacity.

3.0 Objectives of the Electronic Transactions Policy

This Policy is aligned with the objectives of **Vision 2020** and relates specifically to the achievement of the Public Utilities and Infrastructure goals, both of which address Information and Communication Technology, including telecommunications.

The **Vision 2020** Focus on Infrastructure speaks specifically to the National Information and Communication policy objectives, which are to:

- Encourage competition in telecommunications;
- Establish an authority to facilitate information gathering and dissemination systems;
- Decentralize access to information and improve data collection;
- Encourage a culture of research and development;
- Enact legislation to facilitate implementation of the above;
- Amend antiquated laws to support the use of available technology and dissemination of information;
- Encourage the formation of private sector data collection services.

The **Vision 2020** Focus on Public Utilities addresses the Telecommunications policy objectives, which are to;

- Implement the National Information and Communications Technology Plan (2003-2008);
- Improve service standards and accessibility to ICT;
- Develop a high speed National Information Infrastructure.

E-commerce introduces new elements into commercial transactions, which traditionally are based on face-to-face interaction and exchange of paper documents. The legal requirements and traditions that evolved in this traditional commercial environment must be modernized to accommodate the global electronic age. Through this Policy and the Electronic Transactions Bill, the Government is taking action to remove legal barriers to the use of electronic transactions and to avoid new barriers being created.

This Policy aims at increasing consumer confidence and trust and facilitating the creation of an environment that is conducive to the widespread adoption of e-commerce. The objectives of the Electronic Transactions Policy are to;

- **Remove barriers to the use of electronic transactions and signatures:** Government will identify and eliminate barriers to the use of electronic transactions that arise from the use of legislative language that implies paper documents, and will reduce uncertainties related to the enforcement of electronic transactions and to the recognition of electronic signatures.

- **Recognise equivalency of signature and record requirements:** Electronic signatures and records will be treated as the equivalent of traditional signatures and paper records if they meet certain criteria; for example, if an electronic signature is sufficiently reliable for the purpose for which the signature is required or if an electronic record is accessible to be useable for subsequent reference.

- **Establish a regulatory structure** for recognizing trusted third parties and other certifiers of the authenticity of electronic signatures; through co-regulation, Government will rely to a large degree on self-regulation and market forces to promote the establishment of trusted third parties and consumer information and education to ensure that users can assess capacity for reliable signature authentication.

- **Ensure the cross-border recognition and enforcement of electronic transactions and signatures**: Government will seek to avoid the exclusion of signatures authenticated in other

jurisdictions and refrain from imposing unnecessary requirements that delay recognition of authenticated electronic signatures originating in other jurisdictions.

- **Recognise international trade implications that arise from electronic signature authentication laws:** Government will avoid using electronic signature authentication laws to erect non-tariff trade barriers to electronic commerce. When Government acts as a participant in the marketplace, it will avoid market-distorting effects to the maximum extent possible when it chooses electronic authentication requirements for its transactions.

- **Harmonise the laws of Trinidad and Tobago regarding electronic transactions with internationally accepted principles:** by referring to international models and legislation in other jurisdictions, the Government will join the international community; as well, Government will begin the task of dealing with the international problem of unwanted communications or "spam," and laying the base for increased international co-operative enforcement efforts regarding "spam," e-fraud and other forms of "cyber-crime."

- **Respect freedom of contract and parties' ability to vary provisions by agreement:** Electronic transaction laws will permit parties to an electronic transaction to vary the terms of most electronic authentication laws, rules or regulations by mutual agreement.

- **Allow for technological development, including different means of creating and authenticating electronic signatures:** Electronic signature technologies and approaches to authentication will not be "locked in" through legislative fiat, rather government policy and legislation will allow for changing market standards and applications in existing and future technologies.

- **Allow market-driven standards to be determined by the private sector:** The private sector should in most cases determine the acceptability of different technologies for electronic signatures and standards for electronic authentication. Through a co-regulatory approach with the private sector, Government will maintain its traditional role in consumer protection and fraud prevention and will take an active role in providing information to consumers about the reliability of particular technologies.

- **Remove the barriers to the introduction of e-government:** e-government will allow Government to serve citizens better and more efficiently and, at the same time, to enhance transparency, accountability and participatory democracy. In order to effectively implement e-government, legislative authority for electronic transactions with Government and the ability to provide services electronically must be established.

- **Encourage investment and economic participation by appropriate adjustment of legal liabilities for certain participants in the electronic marketplace**: Internet service providers and other intermediaries that act as "mere conduits" for electronic information should be assured that no liability will attach to them for content or data that could incur civil or criminal liability as long as they had no actual knowledge of the alleged activity that was contrary to the law or that they took appropriate action when they learned of it. Similarly, service providers of accredited certificates will not be liable if legal requirements are followed.

- **Enhance consumer trust** by ensuring that consumers are entitled to minimum information regarding transactions conducted over the Internet.

- **Maintain the integrity of e-commerce and the Internet** by establishing civil penalties for certain activities related to unwanted communication or "spam." This Policy and the associated Electronic Transactions Bill will be part of a broad strategy that will include criminal sanctions, codes of conduct, business "best practices" and education of both businesses and consumers to deal with this increasingly critical problem.

The Government recognises that the challenge of providing a regulatory framework that is consistent with international standards, but that at the same time does not inhibit innovation and allows for the working of free market forces that form the foundation of e-commerce. Consequently, there is the need to promote a co-regulatory approach that relies on industry self-regulation guided by broad-based government policy. In the Government's view, a "light-handed" means of governance is appropriate.

A draft Electronic Transactions Bill was developed by the Attorney General's Department in 2001 as part of a legislative package on Electronic Commerce. This was drafted on recommendation of the National E-Commerce Policy Committee. Since then, the Government, through ***fastforward*** and **Vision 2020,** determined that ICT will be a major driver of the social and economic development of Trinidad and Tobago. The 2001 draft legislation is being revisited to ensure compatibility with Government priorities, as well as recent international developments in electronic commerce legislation and technologies.

4.0 Principles

It is the responsibility of Government to provide a stable legal framework that removes existing barriers to trade and communications conducted over electronic networks, and eliminates potential new barriers. The Policy follows the principles of media neutrality, technological neutrality and functional equivalence as described in the Background. This Policy and the accompanying Policy on Data Protection are the first stage of legislative renewal designed to establish that the legal environment necessary to achieve the objectives of ***fastforward*** is in place.

The main body of work that has been recognised as the global standard for electronic transactions policy and legislation is the Model Law on Electronic Commerce, which was developed by the United Nations Commission for International Trade and Law (UNICTRAL). From this model law, the relevant sections on electronic documents have been adapted for our local legislation. Similarly, the UNICTRAL Model Law on Electronic Signatures has had a significant influence on more recent legislation dealing with electronic signatures and is recommended as a base for legislation for Trinidad and Tobago. In drafting the Electronic Transactions Bill, the Government has also drawn upon legislation in other jurisdictions, including Singapore, Bermuda, New Zealand, Australia, Saint Vincent and the Grenadines, Sweden, Denmark, and several Canadian provinces.

4.1 Principle 1: General Provisions

4.1.1 Definitions

"addressee" in relation to an electronic record, means a person who is intended by the originator to receive the electronic record, but does not include a person acting as an intermediary with respect to that electronic record;

"certificate" means an electronic attestation that links certain signature verification data to the signatory and confirms his or her identity;

"certification service provider" means a person who issues certificates for the purpose of electronic signatures or provides other services to the public related to electronic signatures;

"consumer" means any person who enters or intends to enter into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier;

"electronic" means, in relation to technology, having electrical, digital, magnetic, wireless, optical, electromagnetic, biometric, phontonic or similar capabilities;

"electronic agent" means a program or other electronic or automated means configured and enabled by a person that is used to initiate or respond to electronic records or performance in whole or in part without review by an individual at the time of the initiation or response;

"electronic record" means a record created, stored, generated, received or communicated by electronic means;

"electronic signature" means information in electronic form in, attached to, or logically associated with a record that is created or adopted by an individual in order to sign that record;

"individual" means natural person;

"information" includes data, text, images, sounds, codes, computer programs, software and databases and, for greater certainty, includes personal information;

"intermediary" with respect to an electronic record, means a person who, on behalf of another person, sends, receives or stores that electronic record or provides other services with respect to that electronic record;

"Minister" means the Minister to whom responsibility for electronic commerce is assigned, and "Ministry" shall be construed accordingly;

"originator" in relation to an electronic record, means a person by whom, or on whose behalf, the electronic record purports to have been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that electronic record;

"public authority" means Parliament, a Joint Select Committee of Parliament or a committee of either House of Parliament; the Court of Appeal, the High Court, the Industrial Court, the Tax Appeal Board or any court of summary jurisdiction; the Cabinet as constituted under the Constitution; a Ministry or a department or division of a Ministry; the Tobago House of Assembly, the Executive Council of the Tobago House of the Assembly or a division of the Tobago House of the Assembly; a municipal corporation established under the Municipal Corporations Act, 1990; a regional health authority established under the Regional Health Authorities Act, 1994; a statutory body, responsibility for which is assigned to a Minister of Government; a company incorporated under the laws of Trinidad and Tobago that is owned or controlled by the State; a Service Commission established under the Constitution or other written law; or a body corporate or unincorporated that is established by the President's prerogative or by a Minister of Government in his official capacity or by another public authority; and any entity designated as a public authority by order of the Minister;

"record" means any document, correspondence, memorandum, book, plan, map, drawing, diagram, pictoral or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things

"signatory" means an individual who holds a signature-creation device and acts either on his own behalf or on behalf of another person to create an electronic signature;

"transaction" includes a transaction of a non-commercial nature, a single communication, or the outcome of multiple related communications.

4.1.2 Binding the State

This Policy shall bind the State.

4.1.3 Exclusions

Principles 2, 3 and 4 shall not apply to any law requiring writing, or signatures or original documents for

a) making, execution or revocation of a will or testamentary instrument;
b) conveyance of real property or the transfer of any interest in real property;
c) creation, performance or enforcement of an indenture, declaration of trust or power of attorney, with the exception of constructive and resulting trusts;
d) production of documents relating to immigration, citizenship or passport matters; or
e) any other matters that may be determined by the Minister by order.

4.1.4 Removals from the exclusion list

The Minister, by order subject to a positive resolution by Parliament, may make this Policy or Bill applicable to any of the legal requirements listed in paragraphs (a), (b), (c) or (d) of Principle 4.1.3.

4.1.5 Voluntary use of electronic transactions

Nothing in this Electronic Transactions Policy requires a person who uses, provides, accepts or retains information or a document, to use, provide, accept or retain it in an electronic form without the consent of that person.

4.1.6 Consent may be inferred

Consent for the purpose of Principle 4.1.5 may be inferred from a person's conduct if there exists a reasonable assurance that the consent is genuine and that it applies to the information or document.

4.1.7 Express consent required for Government

Notwithstanding Principle 4.1.6, consent by Government or a public authority shall be explicit and cannot be inferred.

4.1.8 Certain legal requirements continue

The Policy does not limit the operation of a law that expressly authorizes, prohibits or regulates the use of information or records in electronic form or requires that information or a record be posted or displayed in a specific manner.

4.2 Principle 2: Requirements for Legal Recognition

4.2.1 Legal recognition of electronic transactions

An electronic record or information to which this Policy applies must not be denied legal effect or enforceability merely because it is in electronic form.

4.2.2 Writing

The legal requirement that a record or information be in writing is satisfied by an electronic record if the electronic record is accessible and capable of retention for subsequent reference.

4.2.3 Provision of information

The legal requirement that information or a record be provided or sent to a person may be met by providing or sending the information or record by electronic means. For greater certainty, information or a record is not provided or sent to a person if it is merely made available for access by the person, for example, on a website, or is not capable of being retained.

4.2.4 Specified non-electronic form

Where the law requires that information or a record be presented in a specified non-electronic form, that requirement is satisfied if the information or record in electronic form is organised in substantially the same way, accessible and capable of retention for subsequent reference.

4.2.5 Original form

Where the law requires information or a record be presented or retained in its original form, that requirement is met by information or record in electronic form if there exists a reliable assurance as to the integrity of the information or record and, if it is to presented to a person, the information or record in electronic form is accessible and capable of retention for subsequent reference.

4.2.6 Whether information or a record is capable of being retained

Information or a record in electronic form is not capable of being retained if the person providing the information or record prevents or does anything to hinder its printing or storage by the recipient.

4.2.7 Criteria for integrity and reliability

The criterion for assessing integrity is whether the information or record has remained complete and unaltered, apart from the introduction of any changes that arise in the normal course of communication, storage and display. Reliability shall be determined in light of all the circumstances, including the purpose for which the information or record was created.

4.2.8 Copies

If information or a record may be provi ded in electronic form, a requirement under law for one or more copies of the information or record to be provided to a single addressee at the same time is satisfied by providing a single copy in electronic form.

4.2.9 Electronically signed message deemed to be original document

A copy of an electronically signed message shall be valid, enforceable and effective as the original of the message.

4.2.10 Retention of electronic records

Where the law requires that certain records or information be retained, that requirement is met by retaining records or information in electronic form.

4.2.11 Admissibility and evidentiary weight of electronic records

An electronic record will not be deemed inadmissible as evidence solely on the ground that it is in electronic form or that, if it is the best evidence, on the ground that it is not in the original form.

4.3 Principle 3: Contract Formation and Default Provisions

4.3.1 Formation and validity of contracts

In the context of contract formation, the fact that the transaction is conducted in electronic form or that information or a record of the negotiation or formation of a contract is in electronic form does not affect its validity.

4.3.2 Electronic expression of offer or acceptance

Unless parties agree otherwise, an offer or the acceptance of an offer or any other matter that is material to the operation or formation of a contract may be expressed by means of information or a record in electronic form, including by an activity in electronic form such as touching or clicking on an appropriately designated icon or place on a computer screen or otherwise communicating electronically in a manner that is intended to express the offer, acceptance or other matter.

4.3.3 Involvement of electronic agents

A contract may be formed by the interaction of an electronic agent and an individual or by the interaction of electronic agents.

4.3.4 Errors that occur while dealing with electronic agents

An electronic contract formed by an individual with an electronic agent of another person is invalid and unenforceable if the individual made a material error in the information or record and the electronic agent did not provide an opportunity to prevent or correct the error and the individual notifies the other person of the error, takes reasonable steps to correct the error, and has not received or used any material benefit or value from the other person.

4.3.5 Attribution of electronic records

An electronic record is attributed to a particular person if it resulted from an action of that person or through an agent or electronic agent of that person.

4.3.6 Acknowledgement of receipt of electronic records
Acknowledgement of receipt will validate an electronic transaction if, before sending an electronic record or information or by means of that electronic record or information, the originator has requested or has agreed with the addressee that receipt of the electronic record or information be acknowledged.

4.3.7 Time of sending of electronic records
Unless the originator and addressee agree otherwise, information or a record in electronic form is sent when it enters an information system outside the control of the originator or, if the originator and the addressee are in the same information system, when the information or record becomes capable of being retrieved and processed by the addressee.

4.3.8 Time of receipt of electronic records
Unless the originator and addressee agree otherwise, if information or an electronic record is capable of being retrieved and processed by an addressee, it is deemed to be received by the addressee when it enters an information system designated or used by the addressee for the purpose of receiving information or records in electronic form of the type sent or, if the addressee has not designated or does not use an information system for the purpose of receiving information or records in electronic form of the type sent, upon the addressee's becoming aware of the information or record in the addressee's information system.

4.3.9 Place of sending and receipt
Unless the originator and addressee agree otherwise, information or a record in electronic form is deemed to be sent from the originator's place of business and is deemed to be received at the addressee's place of business.

4.3.10 Place of business
Unless the originator and addressee agree otherwise, the place of business will be deemed to be the place of business that has the closest relationship to the underlying transaction if a party has more than one place of business or, if there is no underlying transaction, the principal place of business of the originator or addressee of the communication.

4.3.11 Habitual residence
If the originator or addressee of a communication has no place of business, then the habitual residence of the originator or addressee is the relevant criterion for the place of sending and receipt of the communication.

4.4 Principle 4: Electronic Signatures

4.4.1 Electronic signature
Parties to a transaction may agree to the use of a particular method or form of electronic signature, unless otherwise provided by law.

4.4.2 Minimum standards for legally required signatures
Where the law requires a signature of a person, that requirement is met in relation to an electronic record by the use of an electronic signature that meets minimum standards of reliability and integrity or is as reliable as appropriate, given the purpose for which, and the circumstances in which, the signature is required.

4.4.3 Reliability and integrity of electronic signatures
Criteria that shall be used to determine the reliability and integrity of electronic signatures include

a) whether the authentication technology uniquely links the user to the signature;
b) whether it is capable of identifying that user;
c) whether the signature is created using a means that can be maintained under the sole control of the user; and

d) whether the signature will be linked to the information to which it relates in such a manner that any subsequent change in the information is detectable.

4.4.4 Regulations regarding electronic signatures

The Minister may by order make regulations setting out a particular form of electronic signature to meet a specific legal requirement.

4.4.5 Electronic signature associated with an accredited certificate

An electronic signature that is associated with an accredited certificate is deemed to satisfy the requirements set out in Principle 4.4.2 for reliability and integrity.

4.5 Principle 5: Certification Service Providers

4.5.1 Registration of certification service providers

No personal shall offer certification services unless registered with the Minister or with such body as may be designated by the Minister by order and has provided the information required by the Minister by order.

4.5.2. Registry of certification service providers

The Minister or a designated body shall maintain a public registry of certificate service providers that includes the information required by the Minister by order; the registry shall identify those certification service providers that have declared they meet the requirements to issue accredited certificates.

4.5.3 Requirements for a certification service provider that issues accredited certificate

A certification service provider that issues accredited certificates to the public shall conduct is operations in a reliable manner and shall:

a) employ personnel who possess the expert knowledge and experience required for these operations, especially with regard to management, technology and security procedures;
b) apply such administrative and management routines that conform to recognized standards;
c) use trustworthy systems and products that are protected against modification and that ensure technical and cryptographic security;
d) maintain sufficient financial resources to conduct its operations in accordance with these requirements and any other provisions set forth in the Act, and bear the risk of liability for damages;
e) have secure routines to verify the identity of those signatories to whom accredited certificates are issues;
f) maintain a prompt and secure system for registration and immediate revocation of accredited certificates; and
g) take measures against forgery of accredited certificates and, where applicable, guarantee full confidentiality during the process of generating signature creation data;
h) comply with Principle 4.8.2; and
i) comply with any other requirements established by the Minister by order.

4.5.4 Self-Certification of compliance with the requirements for a certification service provider of accredited certificates

A registered certification service provider shall notify the Minister or a designated body prior to offering accredited certificates to the public. The notification shall include a statement of compliance with the requirements set out in Principle 4.5.3.

4.5.5 Notification of compliance shall be renewed annually

A registered certification service provider that issues accredited certificates shall provide annually the Minister or a designated body an updated notification of compliance with the requirements of Principle 4.5.3.

4.5.6 Audit by the Minister

The Minister or a designated body may conduct an audit to substantiate that the certification service provider has been or remains in compliance with the requirements of this Act. In order to perform an audit, the Minister or designated body may employ whatever experts they consider may be required.

4.5.7 Responsibility to co-operate with an audit

A certification service provider shall co-operate with and offer all reasonable assistance to the Minister or a designated body that is conducting an audit and shall make available information necessary to satisfy the Minister or a designated body regarding compliance with the requirements of this Act.

4.5.8 Confidentiality

No person who performs or has performed duties or functions in the administration or enforcement of this Act, including performing an audit pursuant to Principle 4.5.6, shall communicate or allow to be communicated information obtained in the course of performance of duties or functions under the Act to any other person except to law enforcement authorities of the Republic of Trinidad and Tobago or for the purposes of the administration and enforcement of this Act.

4.5.9 Powers of the Minister to deal with failure to meet requirements

Where the Minister or the designated body is satisfied that certification service provider no longer meets the requirements to issue accredited certificates, he may:

1) order the certification service provider to cease any or all of its activities, including the provision of accredited certificates;
2) order certification service provider to be struck from the registry;
3) take any actions that the Minister deems reasonable to ensure that the certification service provider is in compliance with the requirements set out in Principle 4.5.4.
4) make any other order that the Minister deems reasonable in the circumstances including, but not limited to, reimbursement of users of the certification service providers services or public notification of cessation of business.

4.5.10 Recognition of external certification service providers

The Minister by order may recognise certificates or classes of certificates as accredited certificates issued by certification service providers or classes of certification service providers established in any other jurisdiction.

4.5.11 Pseudonyms

Certification service providers may, at the request of a particular signatory, indicate in the relevant certificate a pseudonym instead of the signatory's name.

4.5.12 Additional responsibilities of a certification service provider

A certification service provider shall ensure the operation of a prompt and secure directory of certificate holders and a secure and immediate revocation service that makes it possible to check whether an accredited certificate is revoked, the validity period of the certificate or whether the certificate contains any limitations on the scope or value of the transactions for which the signature can be used.

4.5.13 Immediate revocation upon request

A certification service provider shall revoke a certificate immediately upon the receipt of a request to do so by the signatory or if otherwise warranted in the circumstances. The certification service provider shall ensure that the date and time when the certificate is revoked can be determined precisely.

4.5.15 Liability of certification service provider issuing an accredited certificate

A certification service provider issuing an accredited certificate to the public is *prima facie* liable for any damages or loss caused to anyone relying on such a certificate, due to the certificate provider not having met the requirements set forth in Principle 4.5.3 or Principle 4.4.2 or the certificate, when issued, having contained incorrect information.

4.5.16 Release from liability

The certification service provider issuing an accredited certificate may be exempted from liability if the provider can show that the injury or loss was not caused by its own negligence. The certification service provider is also not liable for damages for an injury or loss arising from the use of an accredited certificate in violation of any limitations of use or scope of transaction clearly stated in the certificate.

4.5.17 Same

The provisions in Principles 4.5.15 and 4.5.16 also apply to a certification service provider that guarantees that the certificates of another service provider are accredited.

4.5.18 Costs of an audit

The Minister may order a certification service provider to pay for the costs reasonably incurred in the performance of an audit and may, by order, set fees for registration pursuant to Principle 4.5.1 and notification of compliance pursuant to Principle 4.5.4.

4.6 Principle 6: Intermediaries and Internet Service Providers

4.6.1 Liability of intermediaries and Internet service providers

An intermediary or an Internet service provider, who merely provides a conduit, should not be liable for the content of electronic records if the intermediary or Internet service provider has no actual knowledge or is not aware of facts that would to a reasonable person indicate a likelihood of civil or criminal liability in respect of material on the intermediary network or who, upon acquiring actual knowledge or becomes aware of such facts, follows the procedures required by Principle 4.6.2 as soon as practicable.

4.6.2 Procedure for dealing with unlawful, defamatory etc. information

If an intermediary or Internet service provider has actual knowledge that the information in an electronic record gives rise to civil or criminal liability or may be reasonably believed to give rise to civil or criminal liability, the intermediary or Internet service provider shall, as soon as practicable

a) notify the Telecommunications Authority of Trinidad and Tobago and, if it considers it appropriate, notify the appropriate law enforcement authority of the relevant information; and
b) where authorised by law, disclose the identity of the person for whom the intermediary was supplying services in respect of the information, if the identity of that person is known to the intermediary; and,
c) where authorised by law, remove the information from any information processing system within the intermediary's control and cease to provide or offer to provide services in respect of that information or take any other action authorized by law.

4.6.3 Role of the Telecommunications Authority of Trinidad and Tobago

Where an intermediary or an Internet service provider has notified the Telecommunications Authority of Trinidad and Tobago pursuant to principle 4.6.2 of information in an electronic record that gives rise to civil or criminal liability or that may be reasonably believed to give rise to civil or criminal liability, the Authority may take such action as it considers reasonable, including

a) notify the appropriate law enforcement authorities; or
b) seek an ex parte order of the court to require removal of the information from the information processing system, disclosure of the identity of the person for whom the intermediary was supplying services or any other action that the court considers reasonable in the circumstances.

4.6.4 Codes of conduct and service standards for intermediaries and Internet service providers

Where the Telecommunications Authority of Trinidad and Tobago has developed a code of conduct and service standards for intermediaries and Internet service providers, the intermediaries or Internet service providers shall comply with the code of conduct or service standards. Compliance with relevant codes of conduct and service standards may be taken into account by courts in determining liability.

4.7 Principle 7: Government and Other Public Authorities

4.7.1 General authorisation

In the absence of a specific legal provision that electronic means may not be used or that electronic means shall be used in a specific way, the Government of Trinidad and Tobago and other public authorities may use electronic means to create, collect, receive, store, transfer, distribute, publish or otherwise deal with records or information.

4.7.2 Forms and filings

Subject to Principle 4.7.1, the authority under any law or regulation to issue, prescribe or in any other manner establish a form or to establish the manner of filing a document or submitting information, includes the authority to issue, prescribe or establish an electronic form, or to establish an electronic manner of filing the document or submitting the information.

4.7.3 Electronic payments to Government

A payment required to be made to the Government of Trinidad and Tobago or to any public authority may be made in electronic form in any manner specified by the Central Bank of Trinidad and Tobago or established by the Minister by order.

4.8 Principle 8: Consumer Protection

4.8.1 Minimum information in e-commerce

Suppliers with a place of business in Trinidad and Tobago or who knowingly use an Internet service provider or intermediary based in Trinidad and Tobago shall provide certain information to consumers regarding an electronic consumer transaction. The information shall include, but not be limited to: the identity, address and phone number of the supplier; the characteristics of the goods or services and their price; the arrangements for payment, delivery or performance; and the existence of a right of withdrawal.

4.8.2 Minimum information regarding electronic signatures

Before entering into a contract regarding the issuance of an accredited certificate, a certification service provider shall inform the party seeking the certificate in writing about the following:

1) the terms and conditions concerning the use of the certificate, including any limitations on its scope or amounts;
2) any requirements concerning storage and protection of the signature-creation data by the signatory;
3) the cost of obtaining and using the certificate and of using the other services of the certification authority;
4) whether the certification authority is accredited under a voluntary accreditation scheme or by an accreditation body in another jurisdiction; and
5) procedures for settlement of complaints and disputes.

4.8.3 Unwanted commercial communications ("spam")

Any person who sends unsolicited commercial communications through electronic media to consumers in Trinidad and Tobago or knowingly uses an Internet service provider or intermediary based in Trinidad and Tobago to send, or who has a place of business in Trinidad and Tobago and sends, unsolicited email to consumers shall provide the consumer with a clearly specified and easily activated option to opt out of receiving future communications.

4.8.4 Right of recission

A consumer who is not provided with the information required by Principle 4.8.1 has the right to cancel the transaction within thirty days provided that the consumer has not received any material benefit from the transaction.

4.9 Enforcement

4.9.1 Failure to provide required information to consumers

Every person commits an offence who fails to provide

a) the information to a consumer required by Principle 4.8.1; or
b) the information and technical capacity required by Principle 4.8.3.

4.9.2 False or misleading information

Every person commits an offence who knowingly

a) files information pursuant to the requirements of this Act that contains false or misleading information;
b) provides a consumer or a user of an electronic signature with false or misleading information.

4.9.3 Obstruction of an audit

Every person commits an offence who, with respect to an audit carried out pursuant to Principle 4.5.6 by the Minister or a body designated by the Minister,

a) knowingly makes any false or misleading statement, either orally in writing to persons carrying out the audit, or
b) otherwise obstructs or hinders them in the conduct of their duties and functions.

4.9.4 Breach of obligations of confidentiality

Every person commits an offence who breaches the confidentiality obligations established by Principle 4.5.8.

4.9.5 Directors and officers

Where a corporation commits an offence under this Act, any officer, director or agent of the corporation who directed, authorized, assented to, acquiesced in or participated in the commission of an offence is a party to and guilty of the offence, and is liable to the punishment provided for the offence, whether or not the corporation has been prosecuted and convicted.

4.9.6 Duties of directors

Every director and officer of a corporation shall take all reasonable care to ensure that the corporation complies with

a) this Act and the regulations made under this Act; and
b) any orders imposed by the Minister or his delegate.

4.9.6 Penalties

Every person who commits an offence under this Act is liable

a) upon indictment, to a fine of not more than XX or to imprisonment for a term of not more than XX years, or both if a individual or a fine of XXXX if a corporation; and
b) upon summary conviction, to a fine of not more than YY or to imprisonment for a term of not more than YY years or both if a individual or a fine of YYYY if a corporation.

5.0 References and Bibliography

1) United Nations Conference on Trade and Development, 'E-Commerce and Development Report 2004', UNCTAD Secretariat, United Nations New York and Geneva
2) United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996), available online at:www.uncitral.org/english/texts/electcom/ml-ecomm.htm
3) United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Signatures with Guide to Enactment (2001). Available Online at:http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf [PDF],
4) *Directive 1999/93/EC on a community framework for electronic signatures* (1999). Available Online http://europa.eu.int/ISPO/docs/policy/docs/399L0093/en.pdf [PDF], The European Parliament and the Council of the European Union
5) Australia, Electronic Transactions Act, 1999.
6) Bermuda, The Electronic Transactions Act, 1999
7) Canada, Report of the Task Force on Spam, "Stopping Spam: Creating a Stronger, Safer Internet," May 2005.
8) Canada, British Columbia, Electronic Transactions Act, Statutes of British Columbia, 2001, chapter 10.
9) Canada, Ontario, Electronic Commerce Act, 2000
10) Denmark,
11) Sweden,
12) Saint Vincent and the Grenadines, Electronic Transactions Act, 2004
13) New Zealand, Ministry of Economic Development, Electronic Transactions At 2002: Plain Language Section by Section Explanation,
14) New Zealand, Ministry of Economic Development, "E-Commerce: Building the Strategy for New Zealand, Progress Report, One Year On, November 2001:
15) Organisation for Economic Co-operation and Development, "The Regulatory Framework for E-Commerce—International Legislative Practice," May 21, 2002.
16) Organisation for Economic Co-operation and Development, *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce* (2000). Available Online http://www1.oecd.org/publications/e-book/9300023E.PDF [PDF],
17) Organisation for Economic Co-operation and Development, Consumers in the Online Marketplace: The OECD Guidelines Three Years Later (2003). Available Online at: http://www.olis.oecd.org/olis/2002doc.nsf/LinkTo/dsti-cp(2002)4-final,
18) The Internet Law & Policy Forum International Consensus Principles for Electronic Authentication, (1999). Available Online at: http://www.ilpf.org/events/intlprin.htm,
19) The Internet Engineering Task Force Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (1999). Available Online at: http://www.ietf.org/rfc/rfc2527.txt..
20) American Bar Association, Digital Signature Guidelines (1996). Available Online at: http://www.abanet.org/scitech/ec/isc/dsgfree.html,
21) The Internet Law & Policy Forum, Legislative Principles for Electronic Authentication & Electronic Commerce, (October 23-24, 1997). Available Online http://www.ilpf.org/groups/principles.htm.