fastforward

Trinidad and Tobago. Accelerating into the digital future.

DRAFT POLICY FOR STAKEHOLDER DISCUSSION

Ministry of Public Administration
& Information

"NATIONAL POLICY ON ELECTRONIC TRANSACTIONS."

November 2004

Version 1.0

Table of Contents

1.0 Background **1**

2.0 Purpose **2**

3.0 Principles **5**

3.1 Principle 1 -- Legal Recognition of Electronic Transactions 5
3.2 Principle 2 -- Writing 5
3.3 Principle 3 -- Delivery 5
3.4 Principle 4 -- Signature 5
3.5 Principle 5 -- Original Form 5
3.6 Principle 6 -- Electronically Signed Message Deemed to be Original Document 6
3.7 Principle 7 -- Retention of Electronic Records 6
3.8 Principle 8 -- Admissibility and Evidential Weight of Electronic Records 7
3.9 Principle 9 -- Formation and Validity of Contracts 7
3.10 Principle 10 – Attribution of Electronic Records 7
3.11 Principle 11 -- Acknowledgement of Receipt of Electronic Records 8
3.12 Principle 12 -- Time and Place of Dispatch and Receipt of Electronic Records 9
3.13 Principle 13 -- Electronic Signature Associated with an Accredited Certificate 9
3.14 Principle 14 -- Authorised Certification Service Providers 9
3.15 Principle 15 -- Liability of Authorised Certification Service Provider 10
3.16 Principle 16 -- Encryption 10
3.17 Principle 17 -- Intermediaries and E-Commerce Service Providers 11
3.18 Principle 18 -- Advisory Board 11

4.0 Glossary **12**

1.0 Background

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 that leverages the power of people, innovation, education, information technology and infrastructure to accelerate social, economic and cultural development for all elements of society. ***fastforward*** complements and builds upon Vision 2020, the national development plan, and will play a central role in Trinidad and Tobago becoming a knowledge-based society and achieving its goal of developed country status by the year 2020.

The objectives of ***fastforward*** are to:

- Provide all citizens with affordable Internet access;
- Focus on the development of children, and skills of adults to ensure a sustainable solution and a vibrant future;
- Promote citizen trust, access, and interaction through good governance; and
- Maximise the potential within all citizens, and accelerate innovation, to develop a knowledge-based society.

Substantial legal and policy change is anticipated as part of Trinidad and Tobago's evolution toward a knowledge-based economy. Liberalisation of the telecommunications industry will take place, rules relating to electronic information handling must be clarified, and citizen privacy and security must be ensured. Consequently, government has an important role to play in ensuring there is a clear and stable policy and a regulatory and legal infrastructure in place that supports the smooth transition and continuous progression of the country's ICT programmes.

The fastforward strategy articulates that in using ICT for improving public sector service delivery, government also has an important role to play in ensuring there is a clear and stable regulatory and legal infrastructure in place that supports a smooth transition and constant evolution of the country's Connectivity Agenda. Legislative Review will be carried out to examine the suitability of current legislation in supporting new levels of electronic transaction making recommendations for areas that need to be addressed and will focus on all aspects of legislation, including the current Telecommunications Act; security privacy and data protection; electronic documents and signatures; intellectual property and protection from inappropriate content on the Internet.

Initial drafting has been completed on The Electronic Transactions Bill to provide the legal framework for electronic transactions. This document provides the principles that will guide the policy for completion of The Electronic Transactions Bill.

2.0 Purpose

This policy is aligned with Vision 2020 and relates specifically to the goals and objectives of the focus on Public Utilities and the focus on Infrastructure both of which addresses Information and Communication Technology inclusive of telecommunications.

The Vision 2020 Focus on Infrastructure addresses the National Information and Communication policy objectives which are;

- 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;

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

This Policy is based upon the Bermuda Model which draws upon a variety of sources including the UNICTRAL Model Law on Electronic Commerce (Parts II and III), and merely establishes the legal principles for the conduct of electronic commerce and the processing of electronic transactions. Notably, the Bermuda Bill lays a foundation for the conduct of electronic transactions on a technology-neutral basis that is sufficiently flexible to embrace new technological developments and contemplates a high degree of self-regulation.

The main purpose of the Electronic Transactions Policy is to provide the legal framework for electronic transactions. This framework seeks to provide the legal principles to regulate the use of electronic documents and electronic signatures. The Policy provides the legal requirements governing records to be prepared in an electronic form and sets out the basic rule that an electronic record is not subject to legal challenge merely because it is in electronic form.

The Policy recognizes that a legally binding document can be crated by use of an electronic signature. The Policy also provides for the formation of contract electronically and communication of electronic records. The Government is empowered under to make regulations relating to the use, import and export of encryption programs and other encryption products, and with respect to the protection of personal data.

Furthermore, the Policy also makes provision for intermediaries and ecommerce service providers, and for the establishment of an Advisory Board to advise Government on the execution of this policy.

There are **18 principles** on which this policy is based which are:

1. **Legal recognition of electronic transactions:** An electronic record in not subject to legal challenge merely because it is in electronic form.

2. **Writing:** The legal requirement for writing is satisfied by an electronic record if the record is accessible and capable of retention for subsequent reference.

3. **Delivery:** Information required by law to be delivered or sent to a person may be delivered or sent by electronic means.

4. **Signature:** Where the law requires a signature of a person, that requirement is met in relation to an electronic record.

5. **Original Form:** Where the law requires information to be presented or retained in its original form, that requirement is met by an electronic record.

6. **Electronically signed message deemed to be original document**: A copy of a digitally signed message shall be valid, enforceable and effective as the original of the message.

7. **Retention of electronic records:** Where the law requires that certain documents, records or information be retained, that requirement is met by retaining electronic records.

8. **Admissibility and evidential weight of electronic records:** An electronic record will not be deemed admissibility in evidence solely on the ground that it is electronic form or that, if it is the best evidence, on the ground that it is not in the original form.

9. **Formation and validity of contracts:** In the context of contract formation the fact that the transaction is conducted in electronic form does not affect its validity.

10. **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.

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

12. **Time and place of dispatch and receipt of electronic records:** The place of business of each of the parties is the governing criterion governing the place and dispatches rather the location of the information processing system.

13. **Electronic Signature Associated with an Accredited Certificate:** An electronic signature that is associated with an accredited certificate issued by an authorised certification service provider is deemed to satisfy Principle 1.

14. **Authorised Certification Service Providers:** The provision of certification services for electronic signatures is not subject to prior authorization however a certification service provider can apply to Government to provide accredited certificates.

15. **Liability of Authorised Certification Service Provider**: By issuing an accredited certificate, an authorised certification service provider is liable to any person who reasonably relied on the certificate.

16. **Encryption:** Regulations shall be developed respecting the use, import and export of encryption programs or other encryption products and prohibiting the export of encryption programs or other encryption products from this jurisdiction generally or subject to such restrictions as may be prescribed.

17. **Intermediaries and E-Commerce Service Providers:** An intermediary is not subject to any civil or criminal liability in respect of any information contained in an electronic record in respect of which the intermediary provides services

18. **Advisory Board:** There shall be an Advisory Board whose functions will be to provide advice to Government on matters connected with the discharge this policy.

3.0 Principles

3.1 Principle 1 -- Legal Recognition of Electronic Transactions

Information shall not be denied legal effect, validity, admissibility or enforceability solely on the grounds that it is;

(a) in the form of an electronic record; or

(b) not contained in the electronic record purporting to give rise to such legal effect, but is referred to in that electronic record.

3.2 Principle 2 -- Writing

Where information is required by law to be in writing or is described in any written law as being written, that requirement or description is met by an electronic record if the information contained in the electronic record is accessible and is capable of retention for subsequent reference.

3.2.1

Clause 3,2 applies whether the requirement for the information to be in writing is in the form of an obligation or the law provides consequences if it is not in writing.

3.3 Principle 3 -- Delivery

Where information is required by law to be delivered, dispatched, posted, given or sent to, or to be served on, a person, that requirement is met by doing so in the form of an electronic record provided that the originator of the electronic record states that the receipt of the electronic record is to be acknowledged and the addressee has acknowledged its receipt.

3.3.1

Clause 3.3 applies whether the requirement for delivery, posting, dispatch, sending or serving is in the form of an obligation or the law provides consequences for the information not being delivered, posted, dispatched, given, sent or served.

3.4 Principle 4 -- Signature

Where the signature of a person is required by law, that requirement is met by an electronic record if;

(a) a method is used to identify that person and to indicate that the person intended to sign or otherwise adopt the information in the electronic record; and

(b) that method is as reliable as is appropriate for the purpose for which the electronic record was generated or communicated, in the light of all the circumstances, including any relevant agreement.

3.4.1

Clause 3.4 applies whether the requirement for a signature is in the form of an obligation or the law provides consequences for the absence of a signature.

3.5 Principle 5 -- Original Form

Where information is required by law to be presented or retained in its original form, that requirement is met by an electronic record if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as an electronic record or otherwise; and

(b) where it is required that information be presented, that information is capable of being accurately represented to the person to whom it is to be presented.

3.5.1

Clause 3.5 applies whether the requirement for the information to be presented or retained in its original form is in the form of an obligation or the law provides consequences if it is not presented or retained in its original form.

3.5.2

For the purposes of sub-clause (a) of Clause 3.5;

(a) the criterion for assessing integrity is whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required is to be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

3.6 Principle 6 -- Electronically Signed Message Deemed to be Original Document

A copy of a digitally signed message shall be 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.

3.7 Principle 7 -- Retention of Electronic Records

Where documents, records or information are required by law to be retained, that requirement is met by retaining electronic records, if the following conditions are satisfied:

(a) the information contained in the electronic record is accessible and is capable of retention for subsequent reference;

(b) the electronic record is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) any information that enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received is retained.

3.7.1

An obligation to retain documents, records or information in accordance with Clause 3.7 does not extend to any information the sole purpose of which is to enable the message to be sent or received.

3.7.2

A person may satisfy the requirement referred to in Clause 3.7 by using the services of any other person, if the conditions set forth in sub-clauses (a), (b) and (c) of Clause 3.7 are met.

3.8 Principle 8 -- Admissibility and Evidential Weight of Electronic Records

In any legal proceedings, nothing in the rules of evidence shall apply so as to deny the admissibility of an electronic record in evidence:

(a) solely on the sole ground that it is an electronic record; or,

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

3.8.1

Information in the form of an electronic record will be given due evidential weight and in assessing the evidential weight of an electronic record, regard shall be had to;

(a) the reliability of the manner in which the electronic record was generated, stored or communicated;

(b) to the reliability of the manner in which the integrity of the information was maintained;

(c) the manner in which its originator was identified; and

(d) any other relevant factor.

3.8.2

This section does not affect the application of sections 40 and 41 of the Evidence Act (which relate to the admissibility of documents produced by computers).

3.9 Principle 9 -- Formation and Validity of Contracts

In the context of 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.

3.9.1

As between the originator and the addressee of an electronic record, a declaration of intention or other statement or delivery of a deed shall not be denied legal effect, validity or enforceability solely on the ground that it is the form of an electronic record.

3.10 Principle 10 – Attribution of Electronic Records

An electronic record is attributable to a person if the electronic record resulted form the action of the person, acting in person, by his agent, or by his electronic agent device.

3.10.1

Attribution may be proven in any manner, including by showing the efficacy of any security procedure applied to determine the person to whom the electronic record was attributable.

3.10.2

Attribution of an electronic record by a person under this section has the effect provided for by law or agreement regarding the security procedure.

3.11 Principle 11 -- Acknowledgement of Receipt of Electronic Records

Clauses 3.11.1 to 3.11.3 of this section apply where, on or before sending an electronic record, or by means of that electronic record, the originator has requested or has agreed with the addressee that receipt of the electronic record be acknowledged.

3.11.1

Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, that is sufficient to indicate to the originator that the electronic record has been received.

3.11.2

Where the originator has stated that the electronic record is conditional on receipt of the acknowledgement, the electronic record is treated as though it has never been sent, until the acknowledgement is received.

3.11.3

Where the originator has not stated that the electronic record is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in sub-clause 3.11.3 (a), may, upon notice to the addressee, treat the electronic record as though it had never been sent, or exercise any other rights the originator may have.

3.11.4

Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related electronic record was received by the addressee, but that presumption does not imply that the electronic record corresponds to the message received.

3.11.5

Where the received acknowledgement states that the related electronic record met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

3.11.6

Except in so far as it relates to the sending or receipt of the electronic record, this section is not intended to deal with the legal consequences that may flow either from that electronic record or from the acknowledgement of its receipt.

3.12 Principle 12 -- Time and Place of Dispatch and Receipt of Electronic Records

Unless otherwise agreed between the originator and the addressee, the dispatch of an electronic record occurs when it enters an information processing system outside the control of the originator.

3.12.1

Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic record is determined as follows:

(a) where the addressee has designated an information processing system for the purpose of receiving electronic records, receipt occurs:

  (i) at the time when the electronic record enters the designated information processing system; or

  (ii) if the electronic record is sent to an information system of the addressee that is not the designated information processing system, at the time when the electronic record comes to the attention of the addressee;

(b) where the addressee has not designated an information processing system, receipt occurs when the electronic record enters an information system of the addressee or otherwise comes to the attention of the addressee.

3.12.2

Sub-clause (3.12.1) applies notwithstanding that the place where the information processing system is located may be different from the place where the electronic record is deemed to be received under sub-clause (3.12.3).

3.12.3

Unless otherwise agreed between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the transaction to which the electronic record relates or, where there is no such transaction, the place of business is presumed to be the principal place of business; or

(b) if the originator or the addressee does not have a place of business, it is presumed to be where the originator or the addressee ordinarily resides.

3.13 Principle 13 -- Electronic Signature Associated with an Accredited Certificate

An electronic signature that is associated with an accredited certificate issued by an authorised certification service provider under section 16 is deemed to satisfy the requirements of sub-clause 3.1 (a) and (b).

3.14 Principle 14 -- Authorised Certification Service Providers

The provision of certification services for electronic signatures is not subject to prior authorization however a certification service provider can apply to Government to provide accredited certificates.

3.15 Principle 15 -- Liability of Authorised Certification Service Provider

By issuing an accredited certificate, an authorised certification service provider is liable to any person who reasonably relied on the certificate for –

(a) the accuracy of all information in the accredited certificate as from the date on which it was issued, unless the authorised certification service provider has stated otherwise in the accredited certificate;

(b) assurance that the person identified in the accredited certificate held, at the time the accredited certificate was issued, the signature creation device corresponding to the signature verification device given or identified in the accredited certificate;

(c) if the authorised certification service provider generates both the signature creation device and the signature verification device, assurance that the two devices function together in a complementary manner, unless the person who relied on the accredited certificate knows or ought reasonably to have known that the authorisation of the certification service provider has been revoked.

3.15.1

An authorised certification service provider is not liable for errors in the information in an accredited certificate where -

(a) the information was provided by or on behalf of the person identified in the accredited certificate; and

(b) the certification service provider can demonstrate that he has taken all reasonably practical measures to verify that information.

3.15.2

An authorised certification service provider that;

(a) indicates in the accredited certificate limits on the uses of that certificate; and

(b) makes those limits known to third parties, is not liable for damages arising from the use of the accredited certificate contrary to those limits.

3.15.3

The limits in sub-clause 3.15.2 may include a limit on the value of transactions for which the accredited certificate is valid.

3.16 Principle 16 -- Encryption

Regulations shall be developed respecting the use, import and export of encryption programs or other encryption products and prohibiting the export of encryption programs or other encryption products from this jurisdiction generally or subject to such restrictions as may be prescribed.

3.16.1

For the avoidance of doubt it is declared that, subject to any regulations made under sub-clause (3.16), it is lawful in this jurisdiction for a person to use any encryption program or other encryption product of any bit

size or other measure of the strength of the encryption provided that it has lawfully come into the possession of that person.

3.17 Principle 17 -- Intermediaries and E-Commerce Service Providers

An intermediary is not subject to any civil or criminal liability in respect of any information contained in an electronic record in respect of which the intermediary provides services, if the intermediary was not the originator of that electronic record and;

(a) has no actual knowledge that the information gives rise to civil or criminal liability;

(b) is not aware of any facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known; or

(c) follows the procedure set out in clause 3.15 if the intermediary;

i. acquires knowledge that the information gives rise to civil or criminal liability; or

ii. becomes aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known.

3.17.1

An intermediary is not required to monitor any information contained in an electronic record in respect of which the intermediary provides services in order to establish knowledge of, or to become aware of, facts or circumstances to determine whether or not the information gives rise to civil or criminal liability.

3.17.2

Nothing in this section relieves an intermediary from complying with any court order, injunction, writ, Ministerial direction, regulatory requirement, or contractual obligation in respect of an electronic record.

3.18 Principle 18 -- Advisory Board

There shall be an Advisory Board whose functions will be to provide advice to Government on matters connected with the discharge this policy.

4.0 Glossary

"accredited certificate" means an electronic record that –

(a) associates a signature verification device to a person;

(b) confirms the identity of that person;

(c) is issued by an authorised certification service provider; and

(d) meets the relevant criteria;

"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;

"authorised certification service provider" means a certification service provider authorised under section 15(2) to provide accredited certificates;

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

"data controller" means a person who, either alone, jointly or in common with other persons, determines the purpose for which and the manner in which any personal data is, or is to be, processed;

"data processor" means a person who processes personal data on behalf of a data controller;

"e-commerce service provider" means a person who uses electronic means in providing goods, services or information;

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

"electronic agent device" 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;

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

"electronic signature" means a signature in electronic form in, attached to, or logically associated with, information that is used by a signatory to indicate his adoption of the content of that information and meets the following requirements-

(i) it is uniquely linked to the signatory;

(ii) it is capable of identifying the signatory;

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

(iv) it is linked to the information to which it relates in such a manner that any subsequent alteration of the information is revealed;

"electronic signature product" means hardware or software, or components thereof, that is intended to be used by a certification service provider for the provision of electronic signature services;

"forge an electronic signature" means -

(a) to create an electronic signature without the authorisation of a certification service provider; or

(b) to create an electronic signature verifiable by an identity certificate in which is listed a person who either does not exist or does not hold an authorised identity certificate;

"identifiable natural person" means a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physiological, mental, economic, cultural or social identity;

"information" includes data, text, images, sounds, codes, computer programs, software and databases;

"information processing system" means an electronic system for creating, generating, sending, receiving, storing, displaying, or otherwise processing 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;

"message" means a digital representation of information;

"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;

"personal data" means any information relating to an identified or identifiable natural person;

"prescribed" means prescribed by regulations made under this Act;

"recipient" means a person who receives or has an electronic signature and is in a position to rely on it;

"record" means that is inscribed or written on a tangible medium or that is stored in an electronic, paper-based or any other medium and is retrievable in text or readable form;

"security procedure" means a procedure, established by law or agreement or knowingly adopted by each party, that is employed for the purpose of verifying that an electronic signature, record or performance is that of a particular person or for detecting changes or errors in the content of an electronic record;

"signature creation device" means unique data, including codes or private cryptographic keys, or a uniquely configured physical device which is used by the signatory in creating an electronic signature;

" signature verification device" means unique data, including codes or public cryptographic keys, or a uniquely configured physical device which is used in verifying an electronic signature;

"writing" or "written" includes any handwriting, typewriting, printing, electronic storage or transmission, or any other method of recording information or fixing information in a form capable of being preserved and converted or printed into text or readable form.