Electronic Transactions Act 2008

A BILL ENTITLED
AN ACT To Facilitate electronic transactions and for connected matters
ENACTING CLAUSE

PART1Preliminary
Short title 1. This Act may be cited as the Electronic Transactions Act, 2008.
[Objects. 2. (1)The objects of this Act are to provide a regulatory framework that
(a)recognizes the importance of the information economy to the future economic and social prosperity of Grenada;
(b)facilitates the use of electronic transactions by means of reliable electronic documents ;
promotesthe development of the legal and business infrastructure necessary toimplement secure electronic commerce;
(d)promotes business and community confidence in the use of electronic transactions;
(e)promotes public confidence in the integrity and reliability of electronic documents and transactions in particular through the use of encrypted signatures to ensure the authenticity and integrity of electronic documents;
(f)establishes uniformity of legal rules and standards regarding the authentication and integrity of electronic documents;
(g)facilitates electronic filing of information with Government agencies and statutory bodies and promotes efficient delivery of Government services by means ofreliable electronic documents
(h)enables business and the community to use electronic communication in their dealings with Government.2
[(2) This Act shall be construed in accordance with the objects set out in subsection (1), taking into account what is commercially reasonable in each case.]
Non 3. This Act does not apply to the transactions specified in the First applicability Schedule to the extent specified in thatSchedule.
Interpreta 4.. In this Act
tion. "accredited certificate" means an electronic record that
(a) associates a signature verification device to a person;
(b) confirms the identity of that person;
(c) isissued by an authorized certification service provider; and
(d) meets the relevant criteria;
"addressee" means a person whothe originator of an electronic document intends to receive the document, but does not include a

person acting as an intermediary with respect to that document;

"authorized certification provider" means a certification service provider authorized under section [18(2)] to provide accredited certificates;

"automated communications device" means a computer program or an electronic or other automated device used to initiate or respond to electronic communications in whole or in part, without review or action by a n individual;

"certificate" means any record that

(a) identifies the entity that issues it;

(b) names or otherwise identifies the signatory or a device (including an automated communications device) under the control of the signatory;

(c) specifies its operational period;

(d) is digitally signed by the entity that issues it;3

(e) contains a public key that corresponds to a private key under the control of the originator of the electronic document to which the certificate relates; and

(f) specifies any other matter required to be specified by regulations made pursuant to section 47;

"certification service provider" means a person who issues certificates for the purposes of electronicsignatures orprovides to the public other services related to electronic signatures;

"Certifying Authority" means the Certifying Authority established under section 42;

"data" includes

(a) material in whatever form stored in an electronic communications system;

(b) the whole or part of a computer program; and

(c) a representation of information orconcepts prepared in a form suitable for processing in an electronic communications system;]

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

"electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities and references to carrying out any act "electronically" shall be similarly construed;

"electronic communication" means information generated, communicated, recorded, stored or displayed by electronic means;

"electronic communications system" means a system for creating,4

generating, sending, receiving, storing, displaying or otherwise processing electronic documents or data;

"electronic document" means informationcreated, , generated, communicated, stored, displayedor processed by electronic means[but not limited to electronic data interchange, electronic mail, telegram, telex or telecopy;

"electronic signature" means information that

(a) is contained in, attached to or logically associated with, an electronic document; and

(b) is used by a signatory to indicate his adoption of the content of that document,

but does not include any signature produced by a facsimile machine or an electronic scanning device;

"encrypted signature" means an electronic signature that is encrypted by means of a private key or other encrypted signature creation device;

"encrypted signature creation device" means

(a) unique data, including codes or private cryptographic keys; or

(b) a uniquely configured physical device,

used by a signatory in creating an encrypted signature;

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

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

"information technology requirements" includes software requirements;

"intermediary", with respect to an electronic record, means a person5 who, on behalf of another person, sends, receives or stores that electronic document or provides other services with respect to that document;

"originator", in relation to an electronic document, means a person by whom, or on whose behalf, the documentpurports 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 document

"person" means

(a) an individual 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 ; and

(b) In relation to an artificial person or corporate entity, means the individual or individuals designated to act on behalf of that entity;

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

"security procedure" means a procedure established by law or agreement or knowingly adopted by each party that is employed for the purpose of

(a) verifying that an electronic signature, record or performance is that of a particular person; or

(b) detecting changes or errors in the content of an electronic record;

"signature" includes

(a) any symbol executed oradopted; or

(b) any methodology or procedure employed or adopted,

by a person with the intention of authenticating a record, including electronic or digital methods;

"signature creation device" means unique data, including codes or private cryptographic keys , or a uniquelyconfigured physical device which is used in verifying an electronic signature;6

"signature verification device" means

(a) unique data, including codes or public cryptographic keys;; or

(b) a uniquely configured physical device,

which is used in verifying an electronic signature;

"signatory" means a person who by means of an encrypted signature creation device has (whether acting himself or through another person, or an automated communications device, acting on his behalf) affixed his encrypted signature to an electronic document;

"traffic data" means information about the communication of data using an electronic communications system, including the

(a) number and kind of communications;

(b) origin of the communication;

(c) destination of the communication;

(d) time when the communication was sentand the time when it was received.

"transaction" includes

(a) any transaction in the nature of a contract, agreement or other arrangement; and

(b) a transaction of a noncommercial nature.

Variation by agreement. 5. As between parties involved in generating, sending, receiving, storing or otherwise processing records, any provision of Part 11 or Part 111 may be varied by agreement of the parties.

Agreement required. 6. (1) Except as provided in Part IV nothing in this Act shall be construed as imposing an obligation on any person to create, give, store or receive any information electronically.7

(2) This Act applies to any transaction between parties each of whom has agreed to conduct the transaction electronically.

(3) The fact as to whether or not a party has agreed to conduct a transaction electronically shall be determined
(a) if the party is the Government, by express stipulation by the Government;
(b) in the case of any other party, by the context and surrounding circumstances , including the party' s conduct.
(4) A party that agrees to conduct a particular transaction electronically may refuse to conduct other transactions electronically.
(5) Except as otherwise provided in this Act, any provision of Part II or Part III may be varied by agreement between the parties to a transaction conducted electronically.

PART 11

Legal Requirements Respecting Electronic Transactions

Validity of 7. For the purposes of any law [in force in Grenada] information electronic shall not be deniedlegal effect, validityor admissibility solely on the
documents. ground that it is
(a) inthe form of an electronic document;
(b)communicated by electronic means; or
(c) referred to but not contained in the electronic document purporting to give rise to that legal effect, if the information referred to is known to and accepted by the party against whom it is relied upon.

Require 8. (1) Where anylaw requiresinformation to bein writing, or refers ment for towritten information, any such information that is given electronically
written shall be taken to be given in writing if
information. (a) when the information was given, it was reasonable to expect that the information would be readily accessible so as to be useable for subsequent reference; and
[(b where the information is to be given to the Government and the Government requires that8
(i) the information be given in a particular way in accordance with particular technology requirements; or
(ii) particular action be taken to verify the receipt of the information,
the Government' s requirement has been met; and
(c) where the information is to be given to a person other than the Government, that person consents to the information being given by means of an electronic communication.
(2) This section applies to a requirement or permission to give information, whether or not any of the words "give", "send", "serve" or any other word is used to designate the requirement or permission.
(3) This section does not affect the operation of any other law that makes provision for or in relation to requiring or permitting information

to be given, in accordance with particular information technology requirements
(a) on a particular kind of data storage device; or
(b)by means of a particular kind of electronic communication.
(4) For the purposes of this section ” giving information” includes the following
(a) making an application;
(b) making or lodging a claim;
(c) giving, sending or serving a notice;
(d) lodging a return;
(e) making a request;
(f) making a declaration;
(g) lodging or issuing a certificate;
(h) making, varying or cancelling an election;
(i) lodging an objection;
(j) giving a statement of reasons.
(5) Where any law referred to in subsection (1) requires more than one copy of the information to be submitted to a person, that9 requirement is satisfied by giving the information to the person electronically in accordance with the provisions of this section.
Electronic 9. Unless otherwise provided by law, parties to a transaction may agree to
the signature. use of a particularmethod or form of electronic signature.
Requirement 10. (1) Where a law requires a person’ s signature other than asignature
for signature. of a witness, that requirement is met by means of an electronic signature
if the information is given electronically and
(a) the electronic signature
(i) adequately identifies the signatory and
adequately indicates the signatory’ s approval of the
information to which the signature relates;
(ii) is as reliable as is appropriate having regard to
the purpose for which and the circumstances in which,
the signature is required, including any relevant
agreement;
(b) in the case of a signature on information to be givento a person, that person consents to receiving the electronic signature.
(2) Subject to subsection (3), an encrypted signature shall be presumed to have satisfied the requirements of subsection(1)(a) and (b) if that signature is
(a) uniquely linked to the person whose signature is required;
(b) capable of identifying that person;

(c) created by using means that the person can maintain under his sole control;
(d) linked to the information to which it relates in such a manner that any subsequent alteration of the information or the signatureis detectable.
(3) Subsection (2) shall not be construed as limiting in any way the ability of any person to
(a) establish in any other manner, for the purpose of satisfying the requirement referred to in subsection (1), the reliability of an encrypted signature or other method of indicating identity and approval;10
(b) adduce evidence of the unreliability of an encrypted signature.
(4) Subsection (1) applies whether the requirement for signature is in the form of an obligation or the law merely provides consequences for the absence of a signature.
(5) In determining whether or to what extent, a certificate or an encrypted signature is legally effective, no regard shall be had to the geographic location
(a) where the certificate is issued or the encrypted signature is created or used; or
(b) of the place of business of the certification service provider or signatory.
(6) This section shall not affect the operation of any other law that requires
(a) information that isgiven electronically to contain
(i) an encrypted signature(however described);
(ii) a unique identification in an electronic form; or
(b)a particular method to be used for information that is given electronically to identify the originator and to show that the originator approved the information given.
Requirement 11. (1) Subject to subsection (2), a legal requirement for a signature or that seal be witnessed is met by means of an electronic signature of a signature or witness if in the case of seal to be witnessed. (a) a signature to be witnessed, the signature is an electronic signature that complies with section 8; and
(b)a signature or seal to be witnessed, the electronic signature of the witness adequately
(i) identifies the witness; and
(ii) indicates that the signature or seal has been witnessed.11
(c) is as reliable as is appropriate given the purpose for

which and the circumstances in which, the signature of the witness is required.
(2) A legal requirement for a signature or seal to be witnessed is not met by means of an electronic signature of the witness unless , in the case of such a signature on information that is required to be given to a person, that person consents to receiving the electronic signature of the witness.
Presumption 12. (1) For the purposes of sections 9 and 10, an electronic signature is
re reliability of is presumed to be as reliable as is appropriate if electronic (a) the means of creating the signature
signature. (i) is uniquely linked to the signatory ; and
(ii) was under the sole control of the signatory;
(b)any alteration to the electronic signature made after the time of signing is detectable; and
(c) in any case where the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.
(2) Subsection (1) does not prevent any person from proving on other grounds or by other means that an electronic signature is, or is not, as the case may require, not as reliable as appropriate.
[(7) An electronic communication that meets the requirements of subsection (1)(a) and (b) shall not be denied legal effect solely on the ground that it is an electronic signature.]
Requirements 13. Where any law requires a document or signature to be made, attested,
for acknowledged, authenticated, notarized or verified, or to be made under oath attestation, oath by any person, that requirement is met if the following are attached to or
etc. of logically associated with the document
documents. (a) the person’ s encrypted signature ;
(b) in the case of a signature or a document requiring a signature, a statement by the person attesting to his identity;12
(c) a statement by the person certifying the performance of all obligations imposed by any other law governing the legal validity of the document; and
(d) all other information required to be included under any other law.
Original form 14. (1) Where any law requires or permits information to be presented
of documents. in its original form or to be made available for inspection , that
  requirement is met where the information is produced electronically if

(a) having regard to all the relevant circumstances at the time, the method of generating the information electronically provided a reliable means of assuring that the integrity of the information is maintained;
(b) when the information was sent, it was reasonable to expect that it would be readily accessible so as to be useable for subsequent reference;
(c) where the information is to be produced to
(i) the Government and the Government requires that an electronic form of the document be produced in a particular way, in accordance with particular information technology requirements or that particular action be taken to verify receipt of the document, the Government' s requirement is met; or
(ii) any other person, that person consents to the document being produced electronically.
(2) Where a law requires comparison of a document with an original document, that requirement is met by comparing the document with an electronic form of the original document if the electronic form reliably assures the maintenance of the integrity of the document.
(3) For the purposes of subsection (1) (a) and (2), the criteria for assessing integrity are
(a) that 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;
(b) the purpose for which the information is produced; and13
(c) any other relevant factor.
Requirements 15. (1) Where any law requires a person to retain information for keeping (whether or not in its original form, in writing or in electronic form) for
information. a specified period, that requirement is satisfied by keeping the information in electronic form if the following conditions are satisfied
(a) when the information was first generated in electronic form, it was reasonable to expect that the information would be readily accessible so as to be useable for subsequent reference;
(b) having regard to all the relevant circumstances when the information was first generated in electronic form, the method of retaining the information in that form provided a reliable means of assuring the maintenance of the integrity of the information so generated;
(c) the traffic data relating to the information is also kept in electronic form during the specific period;

(d) when the traffic data was first generated in electronic form, it was reasonable to expect that it would be readily accessible to be useable for subsequent reference; and
(e) if the law requires the information to be kept in electronic form on a particular form of data storage medium, that requirement is satisfied throughout the specified period.
(2) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions specified that subsection are satisfied.
Admissibility and evidential weight of information given electronically
16. (1) In any legal proceedings, nothing in the rules of evidence shall apply so as to deny the admissibility in evidence of any information given electronically
(a) solely on the ground that the information is given electronically; or
(b) if the information is the best evidence that the person adducing it could reasonably be expected to obtain, on the ground that the information is not in its original form.14
(2) Information in the form of an electronic record shall 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
(i) the electronic record was generated, stored or communicated;
(ii) the integrity of the information was maintained;
(c) the manner in which the originator was identified; and
(d) any other relevant factor.
[(3) This section shall not affect the application of the relevant provisions of the [Evidence Act] relating to the admissibility of computer generated evidence.]
Information required to be served or delivered.
17. (1) Where any law requires or refers to serving or delivering information, that information shall be taken to have been served or be served or delivered, as the case may be, if
delivered. (a) the information is contained in an electronic document sent to the person upon whom such service or delivery is required to be effected; and
(b)that person acknowledges the receipt of the information.
(2) Nothing in this section affects any rule relating to the time for service or delivery of information.
Prescribed Forms.
18. Where any lawrequires a person to provide information in a p8escribed non electronic form, the Minister responsible may make regulations

providing
for an electronic form that is
(a) organized in the same or substantially the same way as the prescribednonelectronic form ;
(b) accessible to the other person so as to be useable for subsequent reference; and
(c) capable of being retained by the other person.15
Electronic 19. Where any law requires that a payment be made to the Government, the
payment. Minister responsible may make regulations
(a)for the purpose of authorizing or facilitating the making of the payment by electronic means;
(b)specifying the manner in which the payment may be made;
for the purpose of securing the integrity, security and confidentiality of the payment by electronic means.
Formation 20. (1) In relation to the formation of contracts, an offer and the and validity acceptance of an offer may be expressed electronically, unless the
of contracts. parties agree otherwise.
(2) As between the originator and the addressee of an electronic document, a declaration of intention or other statement or delivery of a deed shall not be denied legal validity or be unenforceable solely on the ground that it is in an electronic document.
(3) A contract may be formed by the interaction of the automated communications device of each party, even if no individual was aware of or reviewed the actions of the device or the resulting terms and agreements.
(4) Subsection to subsection (5), a contract may be formed by the interaction of an automated communications device and an individual acting on his own behalf or for another person, including an interaction referred to in subsection (5).
(5) The interaction mentioned in subsection (4) is one in which the individual performs actions that the individual
(a) is free to refuse to perform; and
(b) knows or has reason to know will cause the device to complete the transaction.
(6) In the circumstances referred to in subsections (4) and (5), the individual or the person on whose behalf the individual is acting, as the case may be, shall not be bound by the terms of the contract unless, prior to the formation of the contract, those terms were capable of being reviewed by the individual.
General provisions relating to electronic transactions
Attribution 21. (1) Unless otherwise agreed between the originator and the16 of addressee of an electronic document, the originatoris bound by that

electronic document only if the document was sent by him or under his authority.
documents. (2) Subsection (1) shall not affect the operation of a law that makes
provisionfor
(a) conduct engaged inby a person within the scope of the person’s actual or apparent authority to be attributed to another person; or
(b) a person to be bound by conduct engaged in by another person within the scope of the other person’s actual or apparent authority.
(3) An electronic documentbetween an originator and an addressee shall be deemed to be that of the originator if it was sent by an information system programmed to operate automatically by or on behalf of the originator.
(4) As between the originator and the addressee, the addressee shall have the right to assume that an electronic document is being sent by the originator and to act on that assumption if
(a) in order to ascertain whether the document is that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or
(b) the document as received by the addressee resulted from the actions of a person whose relationship with the originator enabled that person to gain access to a method used by the originator to identify electronic documents as his own
(5) Subsection (4) does not apply
(a) as of the time when the addressee has received notice from the originator that the electronic document was not sent by the originatorand had reasonable time to act accordingly; or
(b) in any case falling within subsection (4)(b), at any time when the addressee knew, or ought to have known had he exercised reasonable care or used any agreed procedure, that the electronic document was not sent by the originator.17
(6) An addressee is not entitled to regard an electronic document as being what the originator intended to send if the addressee knew, or ought reasonably to have known had he exercised reasonable care or used an agreed procedure, that
(a) the document was sent in error; or
(b) the transmission of the document resulted in an error in the document as received by the addressee.
(7) The addressee is entitled to regard each electronic document

received as a separate document and to act on that assumption, except to the extent that it duplicates another electronic document and the addressee knew or ought reasonably to have known, had he exercised reasonable care or used any agreed procedure, that the electronic document was a duplicate.

Effect of change or error.

22. (1) This section applies where a change or error occurs in the transmission of an electronic document between parties.

(2) Where there is an agreement between the parties to use a security procedure to detect changes or errors in the electronic document and

(a) only one of the parties has conformed to the procedure; and

(b) the nonconforming party would have detected the change or error had that party also conformed,

the conforming party may avoid the effect of the changed or erroneous electronic document.

(3) A party may avoid the effect of an electronic document that results from an error made by the party in dealing with another person's automated communications deviceif

(a) the device did not provide an opportunity for the prevention or correction of the error; and

(b) the conditions specified in subsection (4) are applicable.

(4) The conditions mentioned in subsection(3) are that, at the time the party learns of the error, that party18

(a) promptly notifies the person of the error and that the party did not intend to be bound by the erroneous document;

(b) takes steps that conform to the person's reasonable instructions for the return or disposal of the consideration (if any) received by the party as a result of the erroneous document;

(c) if no reasonable instructions are given under paragraph (b), takes reasonable steps for the return or disposal of such consideration; and

(d) has not received any benefit or value form such consideration.

(5) Where neither subsection (2),(3) nor (4) applies, the change or error shall have the effect provided for by a contract between the parties or by law, in the absence of such contract.

(6) The provisions of subsections (2), (3) and (4) may not be varied by agreement.

Acknowledgement of receipt

23. (1) The provisions of this section apply where, on or before sending an electronic document, or by means of that document, the

receipt originator requests or agrees with the addressee that receipt of the document is to be acknowledged.
of electronic
document.
(2) 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 reasonably sufficient to indicate to the originator that the electronic document has been received.
(3) Where the originator has stated that the electronic document is conditional on receipt of the acknowledgement, the document is to be treated as though it had never been sent until the acknowledgment is received.19
(4) Subsection (5) applies in cases where
(a) the originator has not stated that the electronic document is conditional on receipt of the acknowledgement; and
(b) the acknowledgement is not received by the originator within the time specified or agreed, or, where no time is specified or agreed, within a reasonable time.
(5) 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 paragraph (a), may , upon notice to the addressee, treat the electronic document as though it had never been sent or exercise any other rights that the originator may have.
(6) An acknowledgement of the receipt given by the addressee to the originator shall be taken as prima facie proof that an electronic document was received by the addressee, but nothing in this subsection shall be construed as implying that the electronic document sent corresponds to the electronic document received.
(7) A statement in an acknowledgement of receipt given by the addressee that the related electronic document meets technical requirements, either agreed upon between originator and addressee or set out in applicable standards, shall be taken as prima facie proof that those requirements have been met.
(8) Except in so far as it relates to the sending or receipt of the electronic document, this section shall not affect the legal

consequences that may flow either from the electronic document or from the acknowledgement of its receipt.

Application of 24. Sections 25 to 27 apply to an electronic communication except to the

Sections 2527 extent that the parties to the electronic communication otherwise agree.

Time 25. (1) The dispatch of an electronic communication occurswhen it20 of dispatch. enters an electronic communications system outside the control of the originator or his agent.

(2) Where an electronic communication enters two or more electronic communicationssystems outside the control of the originator, the electronic communication is taken to be dispatched at the time it enters the first of those systems.

Place of 26. An electronic communication is taken to be dispatched from dispatch. (a) the originator' s place of business; or

(b) if the originator has more than one place of business

(i) the place of business that has the closest relationship with the underlying transaction; or

(ii) if there is no place of business to which sub paragraph (i) applies, the originator' s principal place of business; or

(c)if the originator has no place of business, the originator' s ordinaryplace of residence.

Time of 27. (1) An electronic communication is taken to be received receipt. (a) if an addressee has designated an electronic communications system for the purpose of receiving electronic communications

(i) at the time the electronic communication enters that system; or

(ii) if the electronic communication is sent on an electronic communications system other than the system designated by the addressee, at the time when the electronic communication is retrieved by or comes to the attention of the addressee;

(b) if the addressee has not designated an electronic communications system, at the time when the electronic communication enters an electronic communications system of the addressee or otherwise is retrieved by or comes to the attention of the addressee;

(2) Subsection (1) applies notwithstanding that the place where the electronic communications system is located may be different from the21 place where the electronic communication is taken to be received under subsection (3).

Place of receipt. 28. (1) An electronic communication is taken to be received at
(a) the addressee's place of business; or
(b) If the addressee has more than one place of business
(i) the place of business that has the closest relationship with the underlying transaction; or
(ii) if there is no place of business to which subparagraph (i) applies, the addressee's principal place of business; or
(c) If the addressee has no place of business, the addressee's ordinary place of residence.

PART 111. Conduct of parties in relation to electronic communications and signatures

Conduct of party. 29. (1) In this Part, "relying party" means a person who may act in reliance on the basis of a certificate or encrypted signature.
(2) A relying party shall bear the legal consequences of that party's failure
(a) to take reasonable steps to verify the reliability of an encrypted signature;
(b) where an encrypted signature is supported by a certificate, to take reasonable steps to verify the validity and currency of the certificate and to observe any limitation with respect to the certificate.

Conduct of signatory. 30. A signatory who has an encrypted signature creation device shall
(a) exercise reasonable care to avoid unauthorised use of that device;
(b) forthwith notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of, the signature, if the signatory knows
(i) that the device has been compromised; or22
(ii) of circumstances which give rise to a substantial risk that the device may have been compromised;
(c) where a certificate is used to support an encrypted signature, exercise reasonable care to ensure, throughout the life cycle of the certificate, the accuracy and completeness of all material representations made by the signatory in or in relation to the certificate;
(d) indicate, in any document to which he affixes his encrypted signature, whether he does so in a personal capacityoran official capacity.

Conductof 31. (1) A certification service provider who issues a certificate shall

Certification (a) act in accordance with the representations made by it serviceprovider. with respect to its policies and practices;
(b) exercise reasonable care to ensure, throughout the life cycle of the certificate, the accuracy and completeness of all material representations made by it in relation to the certificate;
(c) provide reasonably accessible means for enabling a relying party to ascertain from the certificate
(i) the identity of the certification service provider;
(ii) that the signatory identified in the certificate had control of the encrypted signature creation device at the time when the certificate was issued; and
(iii) that the encrypted signature creation device was valid at the time when the certificate was issued;
(d) provide reasonably accessible means for enabling a relying party to ascertain from the certificate or otherwise
(i) the method used to identity the signatory;
(ii) every limitation on the purpose or value for which the encrypted signature creation device or the certificate may be used;
(iii) whether the encrypted signature creation device is valid and has not been comprised;23
(iv) every limitation on the scope or extent of liability stipulated by the certification service provider;
(v) the facilities provided for the signatory to give notice pursuant to section 30(b);
(vi) the procedures in place to effect revocation;
(e)provide a means for a signatory to give notice pursuant to section 30(b);
(f) ensure the availability of a timely revocation service;
(g) utilize trustworthy systems, procedures and human resources in performing its services.
(2) For the purposes of this section, in determining whether any systems, procedures or human resources utilized by a certification service provider are trustworthy, regard may be had to
(a) the provider’ s financial and human resources, including the existence of assets and the quality of his hardware and software systems;
(b) the provider’ s procedures for processing certificates and applications for certificates;
(c) the provider’ s retention of records and the availability of information to relying parties and to signatories identified in certificates;
(d) the regularity and extent of audits of the provider’ s

operations by an independent body;
(e) any other relevant factor.
Use and 32. (1) A certification service provider may, at the request of a signatory,
disclosure indicate in the relevant certificate, a pseudonym instead of the signatory' s name.
(2)Where a pseudonym is indicated pursuant to subsection (1), the certification service provider shall disclose the signatory' s name if
(a) requested to do so by a Constable pursuant to a warrant issued by a Justice of the Peace or a court; or
(b) otherwise required to do so by law.24
Recognition 33. (1) In determining whether orto what extent an electronic of foreign document is legally effective, no regard shall be had to the location where
el3ctronic the information was created or used, or theoriginator' s place of documents and business.
signatures. (2 An electronic signature created or used outside Grenada shall have the same legal effect in Grenada as an electronic signature created or used in Grenada if it offers a substantially equivalent level of reliability.
(3) In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of subsection (2), regard shall be had to recognized international standards and to any other relevant factors.
Liability of 34. (1) In this section, "intermediary" means a person who sends,
interme receives or stores an electronic document, or provides other services in relation
diaries. to that documenton behalf of another person.
(2)An intermediary shall not be held liable in any civil or criminal proceedings for any information contained in an electronic document in respect of whichthe intermediary provides services, if the intermediary
(a) is not the originator of the document;
(b) has no actual knowledge of the act or omission that gives rise to the civil or criminal liability, as the case may be, in relation tothe document;and
(c) has no knowledge of any facts or circumstances from which the likelihood of such civil or criminal liability ought reasonably to have been known.
(3) Nothing in this section shall be construed as
(a) requiring an intermediary to monitor any information contained in an electronic document in order to establish knowledge of any act, omission, fact, or circumstances giving rise to civil or criminal liability or imputing knowledge of such liability; or

(b) relieving an intermediary from complying with any law, court order, ministerial direction or contractual obligation in respect of an electronic document.25
(4) Subsection (5) shall apply in any case where, in relation to information contained in an electronic document in respect of which the intermediary provides services, the intermediary has
(a) actual knowledge of the act or omission that gives rise to the civil or criminal liability, as the case may be, in respect of the document; or
(b) knowledge of an facts or circumstances from which the likelihood of such civil or criminal liability ought to have been known.
(5) The intermediary shall forthwith remove the document from any electronic communications system with the intermediary' s control and shall cease to provide services in relation to that document.
(6) An intermediary shall not be liable for any act done in good faith pursuant to the provisions of this section.
Part IV. Obligations in relation to electronic transactions for the supply of goods, services or facilities
Interpre 35. (1) This Part applies only to the formation, by means of electronic
tation and transactions, of agreements for the supply of goods, services or facilities, for the
application sale, hire or exchange, and to the performance of such agreements.
of Part IV. (2) This Part applies to any supplier who
(a) in Grenada, offers goods, services or facilities for sale, hire or exchange, to any person inGrenada; or
(b) whether in or outside of Grenada, offers goods, services or facilities, for sale, hire or exchange, to any person in Grenada.
(3) In this Part
"commercial communication" means any electronic communication which constitutes an offer, for sale, hire or exchange, of goods, services or facilities;
"consumer" in relation to
(a) any goods means
(i) any person who acquires or wishes to acquire goods for hisprivate use or consumption; and26
(ii) a commercial undertaking that purchases consumer goods;
(b) any services or facilities, means any person who employs or wishes to be provided with the services or facilities; and
(c) any accommodation, means any person who wishes to coccupy that accommodation;

“goods” includes all kinds of property other than real property, securities, money
or choses in action;
“personal information” means information about an identifiable individual, Including
(a) information relating to the individual’s race, gender, marital status, nationality or ethnicity, colour, sexual orientation, age, physical or mental health, disability, religion, social or political views, language or birth;
(b) information relating to the individual’s education of the individual’s medical, criminal, credit or employment history;
(c) information about financial transactions in which the individual is or has been involved;
(d) the individual’s address, fingerprints or blood type;
(e) the individual’s name where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal personal information about the individual;
(f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature, or further correspondence that would reveal the contents of the original correspondence;
(g) the views or opinions of any person about the individual;
“supplier” means a person who offers by means of electronic transactions any goods, services or facilities for sale, hire or exchange.
Obligations 36. (1) A supplier shall, on the website where goods, services or facilities27
of supplier are offered for sale, hire or exchange by the supplier, make available to
in conduct of the consumer, the information set out in the Second Schedule.
electronic (2) The supplier shall provide the consumer with an opportunity to do the following , in the following order of sequence
transactions.
(a) review the entire electronic transaction;
(b) correct any errors;
(c) withdraw from the transaction before finally placing an order; and
(d) access electronically and reproduce an accurate summary of the order and the terms, including the total cost relating thereto.
(3) Where a supplier fails to comply with subsection (1) or (2), the consumer is entitled to cancel the transaction within fourteen days after receiving the goods, services or facilities to which the transaction applies.
(4) Where a transaction is cancelled under subsection (3)
(a) the consumer shall return the goods and cease using the services or facilities supplied pursuant to the transaction, as the case may

require;
(b) the supplier shall refund all payments made by the consumer in respect of the transaction.
(5) The supplier shall utilize a payment system that is sufficiently securewith
reference to accepted technological standards at the time of the transaction and the type of transaction concerned.
(6) The supplier is liable for any damage suffered by a consumer due to a failure by the supplier to comply with subsection (5).
Cooling37. (1) Subject to subsections (2) and (4), a consumer is entitled to cancel,
off period without giving any reason and without incurring any charge or penalty, any
transaction or credit agreement for the supply of
(a) goods, within seven days after the receipt of the goods; or
(b) services or facilities, within seven days after the date on which the agreement is made.
(2)This section does not apply to any transaction28
(a) for financial services, including investment services, insurance and reinsurance operations and banking services;
(b) conducted at an auction;
(c) for services which began, with the consumer’ s consent, before the applicable cooling off period specified in subsection (1);
(d) where the price for the supply of the goods, services or facilities in question is dependent on fluctuations in the financial markets and cannot be controlled by the supplier;
(e) where the goods in question
(i) are made to the consumer’ s specifications;
(ii) are clearly personalized;
(iii) are of such a nature that they cannot be returned;
(iv) are likely to deteriorate or expire rapidly;
(f) where audio or video recordings or consumer software are unsealed by the consumer;
(g) for the sale of newspapers, periodicals, magazines or books;
(h) for the provision of gaming or lottery services; or
(i) for the provision of accommodation, transport, catering or leisure services or facilities, which the supplier undertakes to provide (when the transaction is concluded)on a specific date or within a specific period.
(3) Subject to subsection (4), if payment for the goods, services or facilities,
as the case may be, is made prior to a cancellation under subsection (1), the consumer is entitled to a full refund of the payment, and the supplier shall make

the refund with thirty daysafter the date of cancellation.
(4) The only charge that may be levied on a consumer who acts under subsection (1) is the direct cost to the supplier of returning the goods.
(5) Nothing in this section shall be construed to prejudice any other rights that the consumer may have under any other law.
Unsolicited 38. (1) A person who sends unsolicited commercial communications commercial communications to consumers shall give to a consumer to whomany such
communi communication is sent29
cations. (a) the opportunity to decline to receive any further such communications from that person; and
(c) upon request by the consumer, the identifying particulars of the source from which that person obtained the consumer’ s contact information or other personal information.
(2)A person who fails to comply with subsection (1) commits an offence.
(3) No agreement is concluded where a consumer fails to respond to an unsolicited commercial communication.
(4) A person commits an offence if that person sends an unsolicited commercial communication to a consumer who has communicated to that person that the consumer does not wish to receive any such communication.
Supply of 39. (1) Where an agreement is made for the supply of goods, services or
goods, facilities, the supplier shall supply the goods, services or facilities, as the case may
services or require, within the time specified in the agreement or, if no time is specified,
facilities within thirty days after the date on which the agreement is made.
pursuant to (2) If the supplier fails to supply the goods , services or facilities, as
transactions the case may require, within the time required under subsection (1), the
conducted consumer may cancel the agreement seven days after giving notice to the
electronically. supplier of that intention .
(3)Where the supplier is unable to carry out the agreement because the goods, services or facilities are unavailable, the supplier shall
(a) forthwith notify the consumer of the inability; and
(b) within thirty days after becoming aware of the inability, refund any payment made by, or on behalf of, the consumer in respect of the goods, services or facilities.
Provisions 40. No provision in any agreement shall be construed as excluding any rights
of this Part or obligations provided for in this Part.
not excluded

by agreement.
[Complaints 41. A consumer who alleges that a supplier has failed to comply with any of
the provisions of this Part, may make a complaint to the [body charged with30
responsibility for Consumer Affairs] [in accordance with the [Consumer Protection Act].
PART VThe Certifying Authority
Certifying 42. (1) For the purposes of this Act there shall be a Certifying Authority,
which shall have the functions specified in subsection (2).
Authority. (2)‘ The Certifying authority shall be the [Trade Board] or such other
person as the Minister may designate by notice published in the Gazette.
(3) The functions of the Certifying Authority shall be to
(a) issue certificates;
(b) issue and regulate the use of private and public key pairs;
(c) authorize and regulate the issue of certificates by
certification service providers;
(d) authenticate certificates issued by any local or overseas
certification service provider;
(e) provide time stamping services in relation to electronic
documents;
(f) provide application programming interface, including
data encryption, encrypted signatures and digital
envelopes;
(g) carry out any other duties assigned to it under this or any
other enactment.
(4) For the purpose of exercising its functions under this section, the Certifying Authority may
(a) carry out such investigations as may be necessary;
(b) cooperate with any overseas certifying authority in
establishing a system of mutual certification;
(c) issue certification practice statements from time to time;
(d) with the approval of the Minister, make regulations
prescribing
(i) the fees to be imposed for the issue of
certificates, authorizations to certification service
providers and private and public key pairs;31
(ii) the manner of application and the requirements
for authorization of certification service
providers;
(iii) standards and codes of conduct for
intermediaries and certification service

providers.

PART VI General

[Misuse of computer. 43 (1) A person whoknowingly and with intent to commit an offence against this Act, or an offence involving property, fraud or dishonesty, causes a computer to perform any function for the purpose of access to any program or data held in that computer in relation to an electronic transaction , commits an offence.

(2) For the purpose of this section, it is immaterial that the act in question is not directed at

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

(3) For the purposes of this section, a person secures or gains access to any program or data held in a computer if, by causing the computer to perform any function that person

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) causes it to be output from the computer in which it is held, whether by having it displayed or in any other manner.

(4) For the purpose of subsection (3) (c), a person uses a program if the function that the person causes the computer to perform

(a) causes the program to be executed; or

(b) is itself a function of the program.32

(5) For the purpose of subsection (3) (d), that the form in which any program or data output and whether or not it represents a form in which , in the case of a program, it is capable of being executed , or, in the case of data, it is capable of being processed by a computer, is immaterial.]

Restrictions on disclosure of information. 44. (1) Subjectto this Part, no information that

(a) has been obtained under or by virtue of the provisionsof this Act; and

(c) relates to the private affairs of a natural person or to any particular business,

shall, during the lifetime of that person or as long as that business continues to be carried on, be disclosed without the consent of that natural person or the person for the time being carrying on that business.

(2) Subsection (1) shall not apply to any disclosure of

information which is made
(a) for the purpose of facilitating the carrying out of
(i) any functions under Part III;
(ii) prescribed public functions ofany person;
(b) in connection with the investigation of any criminal offence or for the purpose of any criminal proceedings;
(c) for the purpose of any civil proceedings that
(i) relate to the provision of certification or accreditation services;and
(ii) are proceedings to which a person authorized in accordance with Part III is a party.
(3) In subsection (2) (b) “public functions” includes any function conferred by or in accordance with any provision contained in or made under any enactment.
(4) If information is disclosed to the publicin circumstances in which the disclosure does not contravene this section, this section shall not prevent its further disclosure by any person.33
(5) A person who discloses any information in contravention of this section is guilty of an offence and is liable
(a) on summary conviction to a fineof$ [];
(b) on conviction on indictment, to imprisonment for a term of [] or to a fine of$ [] or to both.
(6) The Minister may make regulations prescribing standards for the processing of personal data whether that data originates within Grenada or outside of Grenada.
(7) The regulations may provide for
(a) the registration of the standards by data controllers and data processors;
(b) the establishment of a register that is available for public inspection, showing particulars of data controllers and data processors who have registered the standarda and the dates thereof and the countries in respect of which the registration applies;
(c) the application of the standards to those countries specified in the regulations; and
(d) different standards to be applied in respect of personal data originating from different countries.
(8) A data controller or data processor who registers a standard referred to in subsection (6) shall comply with the standard and any amendments made thereto in respect of any personal data that
(a) originates from a country to which the standard applies; and
(b) is collected by the data controller duritng the period of registration.

(9) A data controller or data processor who contravenes subsection (8) is guilty of an offence and is liable on summary conviction to imprisonment for a term [not exceeding six months] or to a fine not exceeding $[] or both.

Penalties. 45. A person who contravenes any provision of this Act (for which no penalty is provided in this Act) or any regulations made hereunder shall be liable upon conviction before aMagistrate to a fine not exceeding [] dollars or to34 imprisonment for a term not exceeding [ ] or to both such fine and imprisonment;

Offences 46. Where a body corporate commits an offence under this Act and the by offence is proved to have been committed with the consent or connivance of, or bodies to be attributable to any neglect on the part of, any director, manager, company corporate. secretary or other similar officer of the body corporate, or any person purporting to act in any such capacity, that officer or person, as the case may be, as well as the body corporate shall be liable for the offence.

Act binds47.This Act binds the Crown.
Crown.

Regulations. 48. The Minister may make regulations generally for giving effect to the provisions of this Act and, without prejudice to the generality of the foregoing, may make regulations prescribing

(a) methods which satisfy the requirements for an encrypted signature underthis Act;

(b) formats by which information may be communicated electronically, whether or not there exist prescribed non electronic forms;

(c) requirements for certification;

(d) the matters to be specified in a certificate;

(e) procedures for the use, importation or exportation of encryption programs or other encryption devices;

(f) the classes of transactions, documents or rules of law to be excluded from the application of this Act;

(g) any other purpose for the more effective achievement of the objects of this Act.

Minister 49. The Minister may by order subject to affirmative resolution of [ ] may amend penalty or Schedules. (a) increase any monetary penalty of this Act; (b) amendany of the Schedules. 35

FIRST SCHEDULE (Section 3)

Transaction	Extent of exclusion from this Act
1. themaking, execution, alteration or revocation of a Will or testamentary instrument;	Whole Act
2. the conveyance of real property or the transfer of any interest in real property;	Whole Act
3. negotiable instruments;	
4. the creation, performance or enforcement of an indenture, declaration of trust or power of attorney , [other thanconstructive and resulting trusts.]	Whole Act
5. Any procedure governed by the [Civil Procedure Rules] or by rules of court made pursuant to any law.	Whole Act

SECOND SCHEDULE (Section 36)

Information to be made available to supplier to consumers

1. Thefull name of the supplier.
2. The supplier’ s geographical address, website address, email address and telephone number.36
3. The geographical address where the supplier will receive service of legal documents.
4. A disclosure as to whether the entity is incorporated or registered under any law and, where applicable, the supplier’ s registration number and place of registration.
5. Details as to membership in any selfregulatory or accreditation bodies to which the supplier belongs or subscribes and the contact information of such bodies.
6. A description of any code of conduct to which the supplier subscribes and how that code may be accessed electronically by the consumer.
7. A description of the main characteristics of each type ofgoods, service or facility (as the case may be)offered on the website by the supplier , which is reasonably sufficient to enable the consumer to make an informed decision as to the proposed electronic transaction.
8. The full price of the goods, services or facilities, as the case may be, including transportation costs, taxes and any other fees or costs.
9. The method of payment required by the supplier.
10. The terms of agreement, including any guarantees, that will apply to the

transaction, and how those terms may be accessed, stored and reproduced by the consumer electronically.
11. The time within which the goods will be dispatched or delivered, the services
rendered or the facilities made available, as the case may be.
12. The manner and period within which consumerscan access and maintain a full record of the transaction.
13. The return, exchange and refund policy of the supplier.
14. Any dispute resolution code to which the supplier subscribes, and how the text of
that code may be accessed electronically by the consumer.
15. The security procedures and privacy policy of the supplier in respect of payment,
payment information and personal information.

MEMORANDUM OF OBJECTS AND REASONS

The Government recognizes the importance of Information and Communication technologies in
this era of globalization .These technologies are becoming a basic resource needed by all persons
in order to enable them to participate fully in the economic, social and cultural life of their
communities as well as the global community.37
The Government is therefore committed to foster a knowledgebased society in order to
ensure access by all the people to all forms of information and to take advantage of the
opportunities offered by the developments in the Information, Communications and Technology
sector.
This Bill seeks to provide a framework for the conduct of electronic transactions. As stated in the
Objects the Bill seeks inter alia, to provide a regulatory framework to facilitate the use of
electronic documents, promote business and community confidence in the use of electronic
transactions and promote publicconfidence in the integrity and reliability of such document and
transactions .
The Bill also establishes uniform legal rules and standards regarding the authentication and
integrity of electronic documents. Provisions are also made to facilitate electronic filing of
information with Government agencies and statutory bodies and thereby promote the efficient
delivery of Government services bysuch means .