BERMUDA STATUTORY INSTRUMENT

BR 4/2002

ELECTRONIC TRANSACTIONS ACT 1999

1999 : 26

THE CERTIFICATION SERVICE PROVIDERS (RELEVANT CRITERIA AND SECURITY GUIDELINES) REGULATIONS 2002

The Minister of Telecommunications and E-Commerce, in exercise of the powers conferred by sections 20 and 32 of the Electronic Transactions Act 1999, makes the following regulations:—

Citation

1 These Regulations may be cited as the Certification Service Providers (Relevant Criteria and Security Guidelines) Regulations 2002.

Relevant criteria

2 For the purposes of section 20 of the Electronic Transactions Act 1999 the relevant criteria are as prescribed in the Code of Practice set out in the First Schedule to these Regulations.

Security guidelines

3 An authorised certification service provider shall, in addition to satisfying the relevant criteria, comply with the security guidelines set out in the Second Schedule to these Regulations.

Commencement

4 These Regulations come into force on ,2002.

FIRST SCHEDULE (Reg. 2)
CODE OF PRACTICE FOR AUTHORISED CERTIFICATION SERVICE PROVIDERS

Part I Preliminary

PART I
PRELIMINARY

1. INTRODUCTION

1.1 This Code of Practice for Authorised Certification Service Providers (the Code) is issued by the Minister of Telecommunications and E Commerce pursuant to section 20 of the Electronic Transactions Act 1999 (the Act). It forms an integral part of the Authorisation Scheme under the ETA (the Scheme) which the Minister intends to introduce.

1.2 The Code is divided into a number of different Parts. **Part II** covers the Authorisation Process; **Parts III and IV** outline the requirements to be met by those Certification Service Providers (CSPs) wishing to be authorised to issue accredited certificates. **Part V** outlines those requirements that a subscriber of a CSP may be required to adopt if they want their electronic signature to be recognised as directly

equivalent to a written one in certain jurisdictions. **Part VI** outlines the Audit and Compliance Requirements for authorised CSPs. **Part VII** deals with the Revocation and Suspension of Authorisation; **Part VIII** the Conduct of Business by Authorised CSPs and **Part IX** the Requirements for Administration.

1.3 The Minister shall take account of this Code in determining whether to grant authorisations to CSPs under section 20 of the Act and recognition, in the case of external service providers, under section 21 of the Act. Throughout the Code (except where stated) the requirements and criteria for authorisation also apply to such recognition.

1.4 If any Part of this Code is not consistent with any provision of the Act, the relevant provision in the Act will prevail.

1.5 The Minister may consult the Advisory Committee on the Code, authorised and recognised CSPs, and the wider industry in determining any amendments that might be made to the Code.

2. DEFINITIONS AND TERMS

2.1 This Code of Practice uses the definitions given in the Act in particular for *accredited certificate, certification service provider, electronic, electronic agent device, electronic record, electronic signature, electronic signature product, Minister, security procedure, signature creation device and signature verification device.* In addition, this Code of Practice also uses the following definitions:

accredited certificate policy	a certificate policy which incorporates the requirements laid down in Part III and Part IV of the Code of Practice
authorised certification service provider	means a certification service provider (CSP) authorised under section 20(2) to provide accredited certificates
certificate policy	named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements
certification practice statement or 'certification PS'	means a statement issued by the CSP to specify the practices and standards it employs in issuing certificates
external service provider	means a CSP established in a jurisdiction other than Bermuda that is granted recognition under section 21 of the Act
reliance limit	means the monetary limit specified for reliance on an accredited certificate
relying party	recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate
Repository	means an information system for storing and retrieving certificates and other information relevant to certificates
Signatory	means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents

3. REFERENCES

Security Management and Accreditation Standards

3.1 Security Guidelines for Certification Service Providers (December 2001)

3.2 ISO/IEC 17799:2000 Code of Practice for Information Security Management

3.3 BS 7799 Part 2: Specification of an Information Security Management System

3.4 ISO TR 13335 Part 3: Guidelines on the Management of IT Security – Security Management Techniques

3.5 ISO TR 13335 Part 4: Guidelines on the Management of IT Security - Selection of Controls

3.6 BSI-DISC PD3002: BS 7799 Risk Assessment and Risk Management Guidelines *(BS 7799 version of 3.2 above)*

3.7 BSI-DISC PD3005: Selection of BS 7799 Controls *(BS 7799 version of 3.3 above)*

3.8 EA 7/03 EA Guidelines for the Accreditation of bodies operating certification/ registration of Information Security Management Systems

3.10 Web Trust CA Standards and Procedures

Laws and Regulations

3.10 The Electronic Transactions Act (ETA), 1999

3.11 The Computer Misuse Act, 1996

3.12 Standard for Electronic Transactions (the "Standard") 2000

PART II
AUTHORISATION OF CERTIFICATION SERVICE PROVIDERS

4. APPLICATION FOR AUTHORISATION

4.1 A CSP applying to be authorised under the Scheme shall be subject to requirements and criteria defined in this Code and any other conditions set by the Minister under section 21 of the Act. External CSPs wishing to be recognised under the Scheme are required to meet the same requirements and criteria.

4.2 The application form for seeking authorisation under the ETA Authorisation Scheme (or as an externally recognised CSP) can be obtained from—

Ministry of Telecommunications and E-commerce

PO Box HM 101, Hamilton, HM AX, Bermuda

The application form is also available on the Ministry's web site (http://www.mtec.bm).

4.3 The completed application form should be submitted to the Minister with any relevant documents or information. The Minister may request further documents or information as are necessary in support of the application. The Minister may also require external verification, via officals or a third party, of the information or evidence presented.

5. PERIOD OF VALIDITY OF AUTHORISATION

5.1 The validity period of authorisation under the Scheme will be 3 years. During this time the Minister may, in exceptional circumstances (including representations made to her concerning the conduct of the authorised CSP) call upon the CSP to present evidence to demonstrate continued compliance with the Code.

6. RENEWAL OF AUTHORISATION

6.1 This Code of Practice applies to an application for the renewal of authorisation as it applies to a new application.

6.2 The authorised CSP may apply to the Minister for renewal of its authorisation at least 30 days before but not earlier than 90 days before the expiry of the validity of the recognition.

6.3 If the CSP has no intention of renewing its licence, it shall:

a) inform the Minister in writing no later than 90 days before the expiry of its licence;

b) inform all its subscribers in writing no later than 60 days before the expiry of its licence;

c) advertise such intention in the Official Gazette on at least three consecutive occasions at least 60 days before termination of its service;.

d) make arrangements to revoke all accredited certificates, which remain, not revoked or expired, regardless of whether the subscribers have requested revocation, if it intend to terminate its service; and

e) make appropriate arrangements to effect an orderly transfer of any information contained in its repository,

including details of certificates issued and any public-key(s).

7. FEES

7.1 The applicant CSP should ensure that any applicable fee accompanies the completed application form. This applies to the initial application and any renewal sought by the CSP.

7.2 Any fee paid will not be refunded if the application is not approved, withdrawn or discontinued or if an authorisation is suspended or revoked.

8. GENERAL CONSIDERATIONS

8.1 An authorised CSP may appoint agents or sub-contractors to carry out some or all of its operations provided that:

a) the agents or subcontractors are equally capable of complying with the Parts of the Code relevant to their operations, and

b) the authorised CSP is, and remains, responsible for the activities of its agents or subcontractors in the performance or purported performance by them of the functions, powers, rights and duties of the authorised CSP under the Act.

8.2 An authorised CSP shall, if required, make available to the Minister a copy of its own public key certificate that it uses in the process of producing accredited certificates. The Minister shall publish the CSP certificate in the authorised CSP disclosure record maintained by the Minister for that CSP. The disclosure record serves as an additional means for making the CSP certificate available to persons who need to verify the validity of the accredited certificates issued by the CSP for at least 7 years after the CSP concerned has terminated its service.

8.3 Where this Code requires an authorised CSP to record, retain or archive information and records, the CSP shall do so for a period of at least 7 years or for such a longer or shorter period as may be specified by the Minister and in a manner that ensures the security, integrity and accessibility of the information and records for retrieval and inspection.

8.4 An authorised CSP shall comply with all applicable regulations regarding the processing of personal data, including that which may be made under section 26 of the Act.

8.5 If an authorised CSP issues to the public both accredited certificates and non-accredited certificates, it shall publicise the fact that it issues different types and categories of certificates.

PART III
RECOGNITION CRITERIA FOR CERTIFICATION SERVICE PROVIDERS ISSUING ACCREDITED CERTIFICATES

9. GENERAL

9.1 The criteria given in this Part of the Code are those, along with the criteria in Part IV, which a CSP has to meet in order to be authorised.

10. FINANCIAL CRITERIA

10.1 The CSP shall have sufficient financial resources to operate in conformity with the requirements laid down in the Act and this Code. It must intend to be, and to remain, a going concern. This includes having appropriate financial resources and arrangements in place to:

a) manage and maintain adequate support for its operations;

b) install, manage and maintain systems and equipment, which it uses in the delivery of services;

c) employ appropriate personnel, both in terms of quality (skill level) and quantity (number of staff), to support its operations

d) be audited on an annual basis in accordance with generally accepted accounting principles.

10.2 The CSP shall make adequate arrangements against potential claims arising from the accredited certificates that it has issued or plans to issue. Where the CSP issues accredited certificates with specific reliance limits, the liability cover, such as by obtaining insurance, should be sufficient to meet the potential liabilities of the CSP in respect of the reliance limits.

11. PERSONNEL

11.1 The CSP shall take reasonable measures to ensure that every trusted person is a fit and proper person to carry out the duties assigned to them.

11.2 The CSP shall employ trusted personnel who—

a) possess the expert knowledge, experience, and qualifications necessary to carry out their duties for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; and

b) have a good knowledge of the Act and this Code, are trained in the certification practice statements and certificate polices issued by the CSP; are trained to apply administrative and management procedures which are adequate; and in recognised standards (see The Security Guidelines for CSPs).

11.3 In addition, CSPs authorised under section 20 of Act, shall employ trusted personnel who have knowledge of and adhere to the Standard for Electronic Transactions (July, 2000).

12. OPERATIONAL CRITERIA

12.1 The CSP must:

a) demonstrate the reliability necessary for providing certification services;

b) ensure the operation of a secure and immediate revocation service;

c) ensure that the date and time when a accredited certificate is issued or revoked can be determined precisely;

d) verify, by appropriate means in accordance with the relevant Bermudan legislation, the identity and, if applicable, any specific attributes of the entity to which an accredited certificate is issued;

e) use trustworthy systems and products that are protected against modification and ensure the technical and cryptographic security of the processes supported by them;

f) take measures against the forgery of accredited certificates, and in cases where the CSP generates signature-creation data, guarantee confidentiality during the process of generating such data;

g) record all relevant information concerning an accredited certificate for an appropriate period of time (at least 7 years), in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

h) not store or copy signature-creation data of the person to whom the CSP provided key management services;

i) before entering into a contractual relationship with a person seeking an accredited certificate to support his electronic signature, inform that person by a means of

communication of the precise terms and conditions regarding the use of the accredited certificate, including any limitations on its use, and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third parties relying on the accredited certificate.

j) use trustworthy systems to store accredited certificates in a verifiable form so that:

(i) only authorised persons can make entries and changes;

(ii) information can be checked for authenticity;

(iii) accredited certificates are publicly available for retrieval in only those cases for which the certificate holder's consent has been obtained; and

(iv) any technical changes compromising these security requirements are apparent to the operator.

12.2 In applying the criteria in 12.1 the CSP must take account of the criteria given in Part IV and, accordingly, must be able to demonstrate that they can issue an accredited certificate conforming to it.

PART IV
CRITERIA FOR ACCREDITED CERTIFICATES

13. GENERAL

13.1 The criteria given in this Part of the Code set out the requirements that have to be met with respect to the content of a certificate issued for it to be considered an accredited certificate.

14. SPECIFICATION

14.1 Accredited certificates must contain:

a) an indication that the certificate is issued as an accredited certificate;

b) the identification of the CSP and the jurisdiction in which it is established;

c) the name of the signatory or a pseudonym, which shall be identified as such;

d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

e) signature-verification data which correspond to signature-creation data under the control of the signatory;

f) an indication of the beginning and end of the period of validity of the certificate;

g) the serial number or identity code of the certificate;

h) the electronic signature of the CSP issuing it;

i) limitations on the scope of the use of the certificate, if applicable; and

j) limits on the value of transactions for which the certificate can be used, if applicable.

PART V
USER REQUIREMENTS FOR SIGNATURE CREATION AND VERIFICATION

15. GENERAL

15.1 **These requirements are not mandatory for the subscriber of a CSP**. However it should be noted that a subscriber of a CSP may be required to use signature creation devices (ie hardware or software) that conform to the criteria given below if they want their signature to be recognised as directly equivalent to a written one in certain jurisdictions; especially in the European Union. The CSP seeking authorisation should therefore be able to inform their subscribers of such information if they are requested to do so.

16. SIGNATURE CREATION DEVICES

16.1 Signature-creation devices shall, by appropriate technical and procedural means, ensure at the least that the:

a) signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;

b) signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;

c) signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against use by others.

16.2 Signature-creation devices shall not alter the data to be signed and prevent such data from being presented to the signatory prior to the signature process.

17. SIGNATURE VERIFICATION

17.1 During the signature-verification process it should be ensured with reasonable certainty that:

a) the data used for verifying the signature correspond to the data displayed to the verifier;

b) the signature is reliably verified and the result of that verification is correctly displayed;

c) the verifier can, as necessary, reliably establish the contents of the signed data;

d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;

e) the result of verification and the signatory's identity are correctly displayed;

f) the use of a pseudonym is clearly indicated; and

g) any security-relevant changes can be detected.

PART VI

COMPLIANCE AND CSP AUDIT

18. COMPLIANCE REQUIREMENTS

18.1 An applicant must be able to demonstrate as part of the approval process that it is in compliance with:

a) the Security Guidelines for CSPs;

b) the criteria in this Code;

c) its certification practice statement(s); and

d) the Act .

18.2 An applicant shall demonstrate their compliance by providing in their application appropriate evidence, either as the result of a third party audit conducted by a qualified independent audit team or by some other process that is deemed to give an equivalent outcome. Where the

CSP chooses to demonstrate compliance based on a self-audit with supporting documentation (which must be signed off by a senior officer in the company) the Minister reserves the right to employ an independent body to verify this audit.

18.3 Presentation of evidence demonstrating compliance to this Code and to the Security Guidelines must be laid out with reference to each paragraph in the afore-mentioned documents or in any other way deemed as acceptable by the Ministry.

18.4 Failure to demonstrate an appropriate level of compliance shall be a ground for not granting, or revocation of, an authorisation.

PART VII

REVOCATION AND SUSPENSION OF AUTHORISATION

19. REVOCATION OR SUSPENSION

19.1 The Minister may take account of the failure of an authorised CSP to comply with this Code in suspending, revoking or not renewing an authorisation granted to that CSP or a recognition granted to a particular certificate or a type, class or description of certificate issued or is to be issued by that authorised CSP under sections 20 and 21 of the Act, as the case may be.

19.2 The Minister may revoke or suspend the authorisation of a CSP:

a) if the CSP is being or will be wound up;

b) if the CSP has entered into any arrangement with its creditors;

c) if the CSP fails to carry on business for which it was authorised;

d) if the Minister has been presented written evidence to the effect that the CSP or its trusted person has not performed its or his duties efficiently, honestly or fairly; or

e) if the CSP contravenes or fails to comply with any condition.

19.3 The Minister may revoke authorisation of a CSP at the request of that CSP.

PART VIII

CONDUCT OF BUSINESS BY AUTHORISED CSPs

20. MANAGEMENT SYSTEM

20.1 An authorised CSP shall use a management system that is trustworthy for the purposes of performing its services, including managing the delivery of services as well as the technical infrastructure used for the generation, management, issuance, renewal, or revocation of accredited certificates. External service providers are required to have a management system equivalent to that required for authorised CSPs as specified in this section of the Code.

20.2 This trustworthy management system includes the technology used (both hardware and software), as well as the non-technical controls and operational procedures that are designed to ensure that the system will execute its intended functions in a consistent, reliable and dependable manner.

20.3 For a management system to be accepted as trustworthy, an authorised CSP should be able to demonstrate that the mechanisms, procedures and conditions under which the system operates are adequate for the performance of its intended use and functions.

20.4 In the context of a technology neutral approach and taking into account a regime of minimal regulatory intervention and the requirements of the Act, an authorised CSP is free to determine the most appropriate management system, technical infrastructure and solutions to support its business operations.

20.5 Where there is a high risk on specific operational aspects of an authorised CSP, for example, those in relation to security sensitive functions, the authorised CSP is expected to adopt systems and procedures that meet such standards as are widely accepted or recognised worldwide. In addition, as a matter of good practice, an authorised CSP shall perform structured assessments to ascertain the underlying risks of its operations, and implement appropriate security controls for managing and monitoring such risks.

21. TYPES OF CERTIFICATE

21.1 An authorised CSP may issue certificates of the following different levels of assurance:

a) certificates that shall be considered as accredited certificates if they meet the requirements of Part IV of this Code;

b) certificates that shall not be considered as accredited certificates.

21.2 An authorised CSP must associate a distinct certificate policy for each type of certificate issued.

21.3 An authorised CSP must draw the attention of subscribers and relying parties to which of the certificates that it issues is accredited in accordance with the Act and this Code and which are not accredited.

22. ISSUANCE OF CERTIFICATES

22.1 Every authorised CSP shall comply with the requirements of the Act and this Code in relation to the issuing of certificates.

22.2 The certificate must contain or incorporate by reference such information as is sufficient to locate or identify one or more repositories in which notification of the revocation or suspension of the certificate will be listed if the certificate is suspended or revoked.

22.3 Every authorised CSP shall issue certificates in accordance with its applicable certification practice statement.

22.4 The subscriber identity verification method employed for the issuance of certificates must be specified in the certification practice statement for accredited certificates.

22.5 An authorised CSP shall provide a reasonable opportunity for the subscriber to verify the contents of the accredited certificate before it is accepted.

22.6 If the subscriber accepts the issued certificate, the authorised CSP shall publish a signed copy of the certificate.

22.7 Notwithstanding paragraph 22.6 the authorised CSP may contractually agree with the subscriber not to publish the accredited certificate.

22.8 Once an accredited certificate has been issued by the authorised CSP and accepted by the subscriber, the authorised CSP shall notify the subscriber through all reasonable channels within a reasonable time of any fact known to the authorised CSP that affects the validity or reliability of the accredited certificate.

22.9 An authorised CSP shall obtain the consent of the subscriber in respect of any personal information of the subscriber, which the CSP intends to include in the accredited certificate that is to be issued to the subscriber and to be listed in any publicly accessible repository.

22.10 All transactions related to the issuance of an accredited certificate including the date and time shall be recorded.

23. RENEWAL OF CERTIFICATES

23.1 All transactions including the date and time in relation to the renewal of an accredited certificate shall be recorded.

24. SUSPENSION AND REVOCATION OF CERTIFICATES

24.1 An authorised CSP shall be able to revoke and may also be able to suspend accredited certificates.

24.2 An accredited certificate shall contain or incorporate by reference necessary information to locate or identify the repository or repositories in which suspension or revocation notices of the accredited certificate will be published.

24.3 Unless an authorised CSP and its subscriber otherwise agree, the authorised CSP that issues an accredited certificate to the subscriber shall suspend or revoke the accredited certificate within a reasonable time after receiving a request from:

a) the subscriber named or identified in the accredited certificate; or

b) a properly authorised person.

24.4 Within a reasonable time following suspension or revocation of an accredited certificate by an authorised CSP, the authorised CSP shall publish a signed notice of the suspension or revocation (e.g. accredited certificate revocation list) in a repository maintained by it or by an outside organisation on its behalf.

24.5 The exact time of the revocation or suspension by the authorised CSP as well as the allocation of liability for transactions using the accredited certificate in the period between the receipt of the request for revocation or suspension and the time when the accredited certificate is revoked or suspended shall be agreed between the authorised CSP and the subscriber.

24.6 An authorised CSP may temporarily suspend an accredited certificate that it has issued if the authorised CSP has reasonable grounds to believe that the accredited certificate is unreliable, regardless of whether the subscriber consents to the suspension; but the authorised CSP shall complete its investigation regarding the reliability of the accredited certificate and decide within a reasonable time period whether to reinstate the accredited certificate or to revoke the accredited certificate.

24.7 If the authorised CSP considers that an immediate revocation of a accredited certificate issued by it is justified in the light of all the information available to it, the accredited certificate can be revoked, regardless of whether the subscriber has given consent to the revocation.

24.8 In the case of suspension requested by the subscriber or a properly authorised person, the authorised CSP shall check with the subscriber or that properly authorised person whether the accredited certificate to be suspended shall be revoked or reinstated after suspension.

24.9 Whenever an authorised CSP suspends or revokes an accredited certificate, which is issued by it, the authorised CSP shall, within a reasonable time, notify the suspension or revocation of the accredited certificate and provide a record to the subscriber of the accredited certificate or the properly authorised person.

24.10 An authorised CSP shall provide on-line or other facilities for subscribers to report to the authorised CSP incidents affecting their accredited certificates or private keys, for example, keys having been lost or compromised.

24.11 All transactions, including the date and time, in relation to suspension or revocation of accredited certificates shall be recorded.

25. CERTIFICATION PRACTICE STATEMENT

25.1 Any material or significant change to the certification practice statement affecting the compliance of the CSP to the Code shall be referred to the Minister.

25.2 Every authorised CSP must highlight to its subscribers any limitation of their liabilities and, in particular, it must draw the subscribers' attention to the implication of any reliance limits on their accredited certificates.

25.3 The subscriber identity verification method for the issuance, suspension, revocation and renewal of an accredited certificate, must be specified in the certification practice statement.

25.4 A dated copy of the most recent version of the certificate practice statement must be filed with the Minister and published on the CSP's public website.

25.5 Every authorised CSP must log all changes to the certification practice statement together with the effective date of each change.

25.6 An authorised CSP shall keep in a trustworthy manner a copy of each version of the certification practice statement, together with the date it came into effect and the date it ceased to have effect

26. ELECTRONIC SIGNATURE CREATION AND VERIFICATION

26.1 Where electronic signature creation and verification is applicable to the service offerings of the CSP the technical implementation employed by the authorised CSP shall conform to the requirements of the Act, this

Code and the CSP Security Guidelines. This implementation shall be such as to ensure that it is computationally infeasible, based on current standards, for any person other than the person to whom the signature correlates to have created an electronic signature which is verified by reference to the public key listed in that person's accredited certificate.

26.2 The electronic signature on its own should be such as to:

a) ensure that the name or other unique identifiable notation of the person to whom the signature correlates be incorporated as part of the signature and cannot, based on current standards, be replaced or forged; and

b) readily present such indicia of identity to a person intending to rely on the signature.

26.3 The technical implementation should ensure that:

a) the steps taken towards the creation of the signature must be under the direction of the person to whom the signature correlates; and

b) no other person can reproduce the sequence of steps to create the signature and thereby create a valid signature without the involvement or the knowledge of the person to whom the signature correlates.

26.4 The technical implementation should indicate to a relying party whether the document or record that the signature purports to sign has been modified in any way and this indication should be capable of being revealed in the process of verifying the signature.

27. SECURITY GUIDELINES

27.1 An authorised CSP shall ensure that in the performance of its operations and the services it provides materially satisfies the current CSP Security Guidelines. An authorised CSP shall develop, establish and maintain adequate and proper security control within its management system as used for its operations in accordance with generally accepted best security practices (as specified in Guidelines).

27.2 The CSP is required to inform the Minister of any departure from compliance with the CSP Security Guidelines and to demonstrate that it is not material.

27.3 Without prejudice to the generality of situations which the auditor may consider to be material, the following incidents of non-compliance will be considered to be material:

a) any non-compliance relating to the validity of an accredited certificate;

b) the performance of the functions of a trusted person by a person who is not suitably qualified; and

c) the use by an authorised CSP of any system other than a trustworthy system.

27.4 The CSP Security Guidelines shall be interpreted in a manner that is reasonable in relation to the context in which a system is used and is consistent with other legislation.

27.5 The CSP Security Guidelines shall be published on the Ministry's website.

28. INCIDENT HANDLING

28.1 An authorised CSP shall implement an incident management plan that must provide at the least for management of the following incidents:

a) compromise of a subscriber key;

b) compromise of the CSP's key

c) penetration of CSP system and network;

d) unavailability of infrastructure; and

e) fraudulent registration and generation of accredited certificates, accredited certificate suspension and revocation information.

28.2 If any incident referred to in paragraph 28.1 ((b) – (e)) occurs, it shall be reported to the Minister within 24 hours.

29. CONFIDENTIALITY

29.1 An authorised CSP or its agent must keep all subscriber-specific information confidential. Any disclosure of subscriber-specific information by the authorized CSP or its agent must be authorised by the subscriber. This may not apply to subscriber-specific information which:

a) is contained in the accredited certificate for public disclosure;

b) is otherwise provided by the subscriber to the authorised CSP for this purpose;

c) relates to the fact that the accredited certificate has been revoked or suspended and to any non-compliance relating to the validity of an accredited certificate; or

d) relates to an illegal activity under Bermudan law.

PART IX
ADMINISTRATION

30. DISCLOSURE

30.1 An authorised CSP shall submit a yearly progress report to the Minister.

30.2 The progress report shall include information on

a) continued compliance with the Code;

b) the number of accredited certificates issued, suspended, revoked, expired and renewed;

c) system performance and any extraordinary incidents; and

d) changes in the organisational structure of the CSP.

30.3 All current versions of the authorised CSP's applicable certification practice statements together with their effective dates must be published on the CSP's Internet website.

31. DISCONTINUATION OF OPERATIONS OF LICENSED CERTIFICATION AUTHORITY

31.1 If an authorised CSP intends to discontinue its operations, the authorised CSP may arrange for its subscribers to re-subscribe to another authorised CSP.

31.2 The authorised CSP shall make arrangements for its records and accredited certificates to be archived in a trustworthy manner.

31.3 If the records are transferred to another authorised CSP, the transfer must be done in a trustworthy manner.

31.4 An authorised CSP shall:

a) give the Minister a minimum of 3 months' written notice of its intention to discontinue its operations;

b) give its subscribers a minimum of 2 months' written notice of its intention to discontinue its operations; and

c) advertise in such manner as the Minister may determine, at least 2 months' notice of its intention to discontinue its operations.

SECOND SCHEDULE (Reg. 3)
SECURITY GUIDELINES FOR AUTHORISED CERTIFICATION SERVICE PROVIDERS

1. Introduction

1.1 General

1.1.1 These security guidelines sets out the general provisions, standards and procedures to be read and used in conjunction with the specific requirements and conditions set out in section 20 the Electronic Transactions Act 1999 (the Act) and the Code of Practice for Authorised Certification Service Providers (the Code of Practice).

1.1.2 These security guidelines set out the minimum standards, which the Minister expects authorised CSPs to comply within order to meet the requirements and the criteria defined in the Code of Practice.

1.1.3 Under section 21 of the Act external service providers are required to meet the responsibilities and obligations equivalent to those required for authorised CSPs as specified in the Code of Practice as well as the provisions and procedures in this document.

1.2 Standards

1.2.1 The general provisions and procedures outlined in these guidelines are based on a number of internationally recognised technical specifications relating to certification practice statements such as those of the IETF (Internet Engineering Task Force) and European ETSI/CEN standards, in addition to various ISO/IEC standards including the best practice management system standards such as ISO/IEC 17799 and BS

7799 Part 2. They are also formulated to be consistent with the AICPA/CICA Web Trust Program for Certification Authorities.

2. References

2.1 Management and Technical Standards and Specifications

2.1.1 IETF RFC 2527 (1999): "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework", S. Chokhani, W. Ford.

2.1.2 ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8: "Information technology – Open Systems Interconnection - The Directory: authentication framework".

2.1.3 ETSI TS 101 465: Policy requirement for certification authorities issuing qualified certificates

2.1.4 ETSI TS 101 862: Qualified Certificate Profile

2.1.5 ETSI TS 101 861: Time Stamping Profile

2.1.6 ETSI TS 101 733: Electronic Signature Formats

2.1.7 ISO/IEC 17799:2000 Code of Practice for Information Security Management

2.1.8 BS 7799 Part 2: Specification of an Information Security Management System

2.1.9 ISO TR 13335 Part 3: Guidelines on the Management of IT Security – Security Management Techniques

2.1.10 ISO TR 13335 Part 4: Guidelines on the Management of IT Security - Selection of Controls

2.1.11 BSI-DISC PD3002: BS 7799 Risk Assessment and Risk Management Guidelines (BS 7799 version of 3.1.10)

2.1.12 BSI-DISC PD3005: Selection of BS 7799 Controls (BS 7799 version of 3.1.11 above)

2.1.13 tScheme TS042_1.0 Approval Profile for Registration Services

2.1.14 tScheme TS055_1.0 Guidelines for the Verification of Identity of Individuals

2.1.15 tScheme TS056_1.0 Guidelines for the Verification of Identity of Organisations

2.1.16 EA 7/03 EA Guidelines for the Accreditation of bodies operating certification/ registration of Information Security Management Systems

2.1.17 FIPS PUB 140-1 (1994 January 11): "Security Requirements For Cryptographic Modules".

2.1.18 ISO/IEC 15408 (1999): Information technology - Security techniques - Evaluation criteria for IT security (parts 1 to 3)

2.1.19 ANSI X.979 PKI Framework Specification

2.1.20 AICPA/CICA Web Trust Program for Certification Authorities.

2.2 Laws, Regulations and Codes

2.2.1 The Electronic Transactions Act, 1999

2.2.2 The Computer Misuse Act, 1996

2.2.3 Code of Practice for Authorised Certification Service Providers (December 2001)

2.2.4 Standard for Electronic Transactions, May, 2000

3. Management Guidelines

3.1 Accredited Certificate Policy and Certification Practice Statement

3.1.1 The subscribers and relying parties shall be informed of the CSPs accredited certificate policy and certification practice statement and any updates thereafter. The significance and implications of the accredited certificate policy and certification practice statement shall be brought to the attention of the subscriber.

3.1.2 The CSP shall only claim conformance to the Act and the applicable accredited certificate policy if the CSP has been assessed to comply with the requirements and criteria in the Code of Practice.

3.1.3 An accredited certificate policy shall be defined for each class of accredited certificates that have common assurance and requirements. Where applicable this shall also set out any limitations on the usage of each class or description of accredited certificate issued by it, covering for example:

a) usage for which the issued accredited certificates are suitable, e.g. e-mail, retail transactions, contracts, invoices;

b) restrictions on the usage of the issued accredited certificates; and

c) prohibitions on the usage of the issued accredited certificates.

3.1.4 Each accredited certificate policy shall be identified by a unique object identifier (OID), as per the definition and format specified the ISO/ITU standards on OIDs.

3.1.5 The authorised CSP shall provide a summary of the purpose and scope of the certification practice statement. This summary should set out the scope of the authorisation granted by the Minister (including any conditions attached to it) and a general description of what the authorisation such recognition means for both subscribers and relying parties. An authorised CSP may also highlight the scope and the terms and conditions of its services.

3.1.6 An authorised CSP shall identify all known groups or functions that form part of, or participate in, the operation and maintenance of its certification services. For example this may include the subscriber registration function, repositories and target end users (subscribers and rely parties). Where one or more of the core CSP functions are outsourced, such as using third party registration, this must be clearly identified.

3.1.7 An authorised CSP shall provide at least one point of contact for handling enquiries from subscribers on regulatory and other matters. Typically the CSP shall provide as a minimum the telephone number, postal address and e-mail address for this contact point. The authorised CSP shall also provide information on reporting or hotline facilities for subscribers to report lost or compromised keys.

3.2 Duties and Obligations

Authorised CSP

3.2.1 An authorised CSP shall clearly state the duties and obligations it assumes as part of its service offerings, encompassing specific requirements and any conditions for its authorisation set out in the Act and the Code of Practice. Examples of these obligations include:

a) notification (including the timing of such notification) of issuance of a accredited certificate to the subscriber who is the subject of the accredited certificate being issued; and

b) notification (including the timing of such notification) of revocation or suspension of an accredited certificate to the subscriber whose accredited certificate is being revoked or suspended.

c) where an authorised CSP has outsourced any of its functions, the respective duties and obligations of these functions shall be separately described.

Subscriber

3.2.2 An authorised CSP shall describe the duties and obligations on its subscribers including requirements set out in the accredited certificate policies it supports, including, for example:

a) ensuring accuracy of representations in accredited certificate application;

b) protection of the subscriber's private key;

c) restrictions on private key and accredited certificate use; and

d) notification upon compromise or loss of private key.

Relying party

3.2.3 An authorised CSP shall clearly state all representations made to relying parties in accordance with the certification practice statement, including any accredited certificate policy it supports, including for example:

a) understanding the purpose for which the accredited certificate is used;

b) responsibilities over the verification of digital signature;

c) responsibilities over the checking of certification revocation and suspension; and

d) acknowledgement of applicable liability limitations and warranties.

Repository

3.2.4 An authorised CSP shall clearly state the obligations it assumes in relation to any repository service it might provide, encompassing specific requirements and any conditions for its authorisation set out in the Act and the Code of Practice. Examples of such obligations include the timely publication of accredited certificates and revocation (including accredited certificate suspension as appropriate) information, and the terms of accessibility and availability of the repository.

3.3 Liability

3.3.1 With respect to each accredited certificate that an authorised CSP issues, it shall clearly specify:

a) any warranties and/or limitations it may want to impose;

b) the extent of liability that it covers (e.g. direct, indirect, special, consequential, incidental and liquidated damages) and any disclaimers and limitations on its obligations;

c) any limitations on losses per accredited certificate or per transaction; and

d) additional exclusions that may be applicable.

3.4 Financial Responsibility

3.4.1 An authorised CSP shall specify aspects relating to its financial responsibilities and any other parties identified in the certification practice statement. Areas that may be addressed include:

a) whether any fiduciary relationships exist between any parties identified in the certification practice statement or any other interested parties as a result of the act of issuance of accredited certificates;

b) financial assurances provided by the authorised CSP to subscribers and relying parties in respect of its potential or actual liabilities and claims against reliance limits on its accredited certificates; and

c) any other financial aspects such as existence of performance bonds, insurance policies or any other responsibilities that may arise from the authorisation process as a condition of authorisation.

3.5 Interpretation and enforcement

Governing law

3.5.1 The CSP shall state in its certification practice statements, subscriber agreements and relying party agreements the applicable governing law. This is particularly relevant to those CSPs that are recognised under Section 21 of the Act.

Dispute resolution procedures

3.5.2 An authorised CSP shall state the procedures it will use to resolve disputes and claims regarding its operations and representations to its subscribers or relying parties of the accredited certificates it offers. The procedures shall state at a minimum the process of filing a dispute or claim with it and the steps it takes upon notification of a claim or dispute. Examples of such procedures can be found in the standards and procedural documents supporting other similar national legislation such as the Electronic Transactions (Certification Authority) Regulations 1999 of Singapore.

3.6 Fees

3.6.1 An authorised CSP shall clearly state all the fees it will charge for its certification services with respect to any accredited certificates issued directly to the public.

3.7 Publications and Repositories

3.7.1 An authorised CSP shall specify the policy and mechanism that it has implemented to provide its subscribers and relying parties with the information relating to its accredited certificates, its certification practice statement (including the details of any certification policies that it supports), and its current recognition status and the recognition status of the accredited certificates it issues. An authorised CSP should state, at a minimum, the means and frequency of publication, the availability of the information, and any controls over access and details of the repository (if provided).

3.7.2 Reference to the certification practice statement shall be displayed prominently on the web page of the authorised CSP.

3.7.3 Since the procedures followed by an authorised CSP are expected to evolve, updates to the certification practice statement shall be published as soon as practicable. All changes shall be prominently displayed at the same locations where the certification practice statement is displayed and referred to the Minister.

3.8 Confidentiality Policy

3.8.1 An authorised CSP shall specify its policy on maintaining confidentially of information, including for example:

a) types of information that must be kept confidential by the authorised CSP, including any outsourced functions;

b) types of information that is not considered confidential;

c) the persons that are entitled to be informed of reasons for revocation and suspension of accredited certificates:

d) policy on release of information, e.g. to law enforcement officials, requirement to provide evidence for legal proceedings, etc;

e) conditions upon which the authorised CSP, including any outsourced functions, may disclose records and information upon owner's request/consent; and any other circumstances under which confidential information may be disclosed.

3.8.2 Authorised CSPs shall comply with the applicable data protection provisions in the Standard for Electronic Transactions, 2000, and any applicable regulations regarding the same made under section 26 of the Act.

3.9 Intellectual Property Rights

3.9.1 An authorised CSP shall address any intellectual property rights related to the content of accredited certificates, revocation/validity information of accredited certificates, certification practice statement, and certificate policies.

3.10 Security and Risk Management

3.10.1 An authorised CSP shall adopt a security policy in accordance with generally accepted best practices (see section 6).

3.10.2 An authorised CSP shall establish a comprehensive security incident reporting and handling procedure, and a business continuity disaster recovery set-up and procedure for its operation.

3.10.3 An authorised CSP shall adequately identify and establish procedures to deal with the risks associated with its operation. It shall implement a risk management plan that will provide for the management of, including without limitation, the following incidents:

a) key compromise;

b) security breach of the system or network of the authorised CSP;

c) unavailability of the infrastructure of the authorised CSP; and

d) unauthorised generation of accredited certificates and of accredited certificate suspension and revocation information.

4. Accredited certificate management guidelines

4.1 Management Procedures and Processes

4.1.1 An authorised CSP shall maintain effective procedures and controls over the management of certificates in accordance with the best practice given in these Guidelines; including but not limited to the following examples:

a) before issuing or renewing a accredited certificate, an authorised CSP shall verify the identity of the person who applies for the issuance or renewal of a accredited certificate in accordance with procedures stated in the relevant certification practice statement;

b) the authorised CSP shall also verify the uniqueness of the person's name (taking into account section 22 of the Act for the use of pseudonyms);

c) there shall be appropriate procedures to notify subscribers of the need to renew their certificates prior to the expiry of their certificates;

d) an authorised CSP shall adopt an open and common interface (i.e. the interface should be some form of common or standardised interface that all authorised users can have access to so that a user does not need to rely on special arrangements to get access to certificates) for the issuance of its accredited certificates; the format of the certificate shall be stated in the relevant certification practice statement;

e) there are proper policies and procedures in place to ensure that the performance of the repository meets the service levels set out in the certification practice statement of the CSP; and

f) an authorised CSP shall set out in its certification practice statement procedures for subscriber complaints.

Note: Key-roll over (see section 4.5) is not considered to be a procedure covered by 4.1.1 (a) above

Certificate Issuance

4.1.2 An authorised CSP shall specify the specific process it adopts for issuing accredited certificates. The process for issuance of accredited certificates may include:

a) the generation of keys;

b) delivery of keys to the appropriate parties;

c) generation of accredited certificates;

d) delivery of accredited certificates; and

e) posting of the accredited certificates to a repository.

Certificate Acceptance

4.1.3 An authorised CSP shall define the technical or procedural process to

a) explain to subscribers their responsibilities as defined in section 3.2.2;

b) inform subscribers that their accredited certificates have been issued ;

c) allow the subscribers to accept or reject the accredited certificates; and

d) enable the subscribers to obtain the accredited certificates.

Revocation request

4.1.4 An authorised CSP shall specify the process for authenticating and handling revocation requests, covering for example:

a) who is authorised to request revocation of an accredited certificate and under what conditions;

b) the effect of a revocation;

c) how soon will the validity status of accredited certificates be published after revocation;

d) the responsibilities of the subscriber regarding the report of events requiring revocation; and

e) protections afforded to the subscriber once revocation is requested including the allocation of liability between the authorised CSP and the subscriber.

Suspension request

4.1.5 An authorised CSP shall specify whether it supports the suspension of accredited certificates, and if so shall detail the conditions for, as well as the effect of a suspension. It shall be specific about the implementation of suspensions and, if appropriate, address the same elements identified for revocations in section 4.7.3.

4.2 Registration, Identification and Authentication

4.2.1 An authorised CSP shall verify by appropriate means the identity, and if applicable, any specific attributes of the subscriber to which the accredited certificates is issued. Where a physical identification is involved this information shall be checked against the physically present person (either directly or indirectly through submitted documentation which provides equivalent assurance). Checks using documentation (paper or electronic) should at least verifies the subscribers:

a) full name (including family and first names);

b) physical address at which the subscriber can be contacted;

c) data and place of birth (for members of the public);

d) for members of the public a nationally recognised identity number or other attributes that may be used to, as far as possible, distinguish the person from others with the same name.

4.2.2 An authorised CSP shall specify the procedures that it uses, or those of its outsourced registration function if appropriate, to identify and authenticate a subscriber prior to the issuance of accredited certificates in accordance with 4.2.

4.2.3 An authorised CSP shall set out the identification and authentication procedures and the naming conventions to be followed in the issuance of new accredited certificates. An authorised CSP shall cover the specific procedures that it follows in order to identify the accredited certificate applicant in accordance with 4.2 above, including the specific documents that an individual or organisation must produce prior to the authorised CSP issuing an accredited certificate to the end entity.

Naming principles and conventions

4.2.4 An authorised CSP shall specify the naming convention that its has adopted to ensure that the accredited certificate of a person can be unambiguously identified. An example of such a convention would be the X.500 Distinguished Names (DN) convention.

4.2.5 An authorised CSP shall specify whether names within an accredited certificate must be meaningful (i.e. using commonly understood semantics to describe the identity of the person or organisation) and if so, its procedures for ensuring that the DNs assigned to its subscribers are meaningful and appropriately identify the subscriber.

4.2.6 An authorised CSP shall provide guidance on the interpretation of the name formats contained within the accredited certificates issued under the certification practice statement. In general, if the interpretation of names within an accredited certificate may be misconstrued by relying parties, the authorised CSP shall provide guidance to relying parties to reduce the risk of misinterpretation.

4.2.7 An authorised CSP shall specify if names within accredited certificates are required to be unique and its requirements or any uniform rules that are applied for ensuring distinguished names are classed as unique.

4.2.8 If appropriate, an authorised CSP shall specify procedures for resolving any naming conflicts.

Proving possession of private key

4.2.9 If subscribers generate their own key pairs and they remain in exclusive control of the private keys, an authorised CSP must state how it checks and assures itself that the subscriber's private key corresponds to the public key submitted for certification.

Authentication of subscriber identity

4.2.10 An authorised CSP shall specify the process it uses for ensuring that the name on an accredited certificate corresponds to the person being issued the accredited certificate. The information will enable subscribers to understand the requirements necessary for obtaining an accredited certificate under the certification practice statement and will enable relying parties to understand and draw conclusions as to the reliability of the accredited certificates issued under the certification practice statement.

4.3 Issuance of Certificates

a) An authorised CSP may issue an accredited certificate to a person only after it has:

   (i) received a request for issuance of the accredited certificate from the person applying for such a certificate or another authorised to do so on their behalf; and

   (ii) complied with all of the practices and procedures set out in the certification practice statement including procedures regarding identity verification of the person in respect of that type, class or description of accredited certificates.

b) An authorised CSP shall provide a reasonable opportunity for the subscriber to verify the contents of the accredited certificate before accepting the certificate.

c) An authorised CSP shall publish accredited certificates that it issues and that are accepted by its subscribers in the on-line and publicly accessible repositories maintained by it or maintained for it by one or more third parties.

d) An authorised CSP shall obtain the consent of the subscriber in respect of any personal information of the subscriber, which the CSP intends to include in the certificate that is to be issued to the subscriber and to be listed in an on-line and publicly accessible repository.

e) Once an accredited certificate has been issued by the authorised CSP and accepted by the subscriber, the authorised CSP shall notify the subscriber through all reasonable channels within a reasonable time of any fact known to the authorised CSP that affects the validity or reliability of the accredited certificate.

f) An accredited certificate shall state when its validity expires.

g) By issuing an accredited certificate, an authorised CSP represents to any person who reasonably relies on the accredited certificate or an electronic signature verifiable by a public key listed in the accredited certificate that the authorised CSP has issued the accredited certificate in accordance with its applicable certification practice statement.

h) All transactions related to the issuance of an accredited certificate including the date and time shall be recorded.

4.4 Renewal of Accredited Certificates

4.4.1 An accredited certificate is subject to renewal upon expiry of its validity at the request of the subscriber and the discretion of the authorised CSP.

4.4.2 All transactions including the date and time in relation to the renewal of an accredited certificate shall be recorded and digitally signed.

4.5 Routine Rekey

4.5.1 An authorised CSP shall describe the procedures it adopts for routine rekey and certification renewal, in particular if these procedures for identification of the subscriber differ from those used for initial registration and certification issuance. An authorised CSP shall state whether certification renewal takes place without rekeying in its certification practice statement.

4.6 Rekey after revocation

4.6.1 An authorised CSP shall specify the procedure it shall use when issuing a replacement for the accredited certificate after its revocation.

4.7 Certificate Suspension and Revocation

4.7.1 An authorised CSP shall specify the procedures for suspending or revoking an accredited certificate, namely it shall set out the procedures for a subscriber or a properly authorised person to instruct it to suspend or revoke an accredited certificate.

Suspension

4.7.2 An authorised CSP shall provide the details of the suspension process, including the:

a) conditions for suspension (including, but not limited to, who can trigger/recall a suspension);

b) means for requesting/triggering a suspension;

c) means for notification of a suspension (e.g. through postings, electronic mail or inclusion in a accredited certificate revocation list);

d) conditions, such as time limits, for recalling the suspension or moving from suspension to revocation;

e) time for the authorised CSP to suspend a recognised accredited certificate as well as the allocation of liability for transactions using the accredited certificate in between the time when suspension is requested by the subscriber or a properly authorised person, and the time when the accredited certificate is actually suspended;

f) expected time period within which the authorised CSP checks with the subscriber or the properly authorised person whether the accredited certificate that was suspended should be revoked or should be reinstated after suspension; and

g) action the authorised CSP takes in the event that it is not possible for it to contact the subscriber or the properly authorised person to ascertain the ultimate disposition of the suspended accredited certificate.

Revocation

4.7.3 An authorised CSP shall provide the details of the revocation process, including the:

a) conditions for revocation (including, but not limited to, who can trigger/recall a revocation);

b) means for requesting/triggering a revocation;

c) means for notification of revocation (e.g. through postings, electronic mail, inclusion in a accredited certificate revocation list, or updates to a revocation/validity information server); and

d) time for it to revoke an accredited certificate as well as the allocation of liability for transactions using the accredited certificate in between the time when revocation is requested by the subscriber or a properly authorised person, and the time when the accredited certificate is actually revoked.

4.7.4 The subscriber or a properly authorised person may request revocation of the subscriber's accredited certificate using an interface that identifies the accredited certificate to be revoked, explains the reason for revocation, and allows the request to be authenticated (e.g.

digitally or manually signed). Authentication of accredited certificate revocation requests is important to prevent malicious requests of revocation of accredited certificates by unauthorised parties. The means for transmitting the request shall be readily available to the subscriber and the properly authorised person; such as electronic mail and web interfaces.

4.7.5 Typically, a accredited certificate shall be revoked under the following circumstances:

a) identification information or attributes in the user accredited certificate change before it expires;

b) the accredited certificate subject is known to have violated the stipulations of the corresponding CPS;

c) the subscriber suspects or confirms compromise of the private key; or

d) the subscriber no longer wants or requires the ability to sign electronic messages.

Certificate revocation lists

4.7.6 Certificate Revocation Lists (CRLs) identify unexpired accredited certificates that are no longer valid and may also give the reason why each accredited certificate was revoked. An authorised CSP shall state the mechanisms used to distribute the CRLs and how relying parties may access such lists or other mechanisms to establish the status of a particular accredited certificate.

4.7.7 An authorised CSP shall specify the frequency for updating CRLs. It may decide to use or support additional mechanisms for verifying accredited certificate validity. It shall address the available mechanisms, the terms and conditions for their use and how to access the information.

CRL checking requirements

4.7.8 An authorised CSP shall notify subscribers and post prominently in a location generally accessible that there are risks in relying on a digital signature if the accredited certificate containing the public key used to verify the digital signature is no longer valid.

5. Key management guidelines

5.1 Key Management Procedures

5.1.1 An authorised CSP shall maintain effective procedures and controls of its cryptographic key management: over the generation, storage, backup, recovery, distribution, use, destruction, and archiving

of the authorised CSP's own keys including without limitation the following.

a) controls over the use of cryptographic modules for key generation, including the adoption of technical solutions with appropriate security standards;

b) operational controls over key generation including without limitation to ensure:

   (i) the integrity of equipment used in the generation of the keys;

   (ii) that the keys are generated by authorised personnel in a controlled manner; and

   (iii) where subscriber key pairs are generated by the authorised CSP, procedures shall be established to ensure that the private key is delivered to the subscriber in a secure manner without being tampered with; once the private key is delivered to the subscriber, the authorised CSP shall not maintain a copy of the subscriber's private key without the legal authorisation and consent of the subscriber;

c) controls over key storage, backup and recovery including without limitation

   (i) regular and vigorous testing of the authorised CSP's recovery procedures;

   (ii) procedures to ensure safe custody of the authorised CSP's private key, such as by placing it under dual access control. Appropriate measures shall be established to detect any unauthorised attempts to access the key; and

   (iii) procedures to ensure that the backup of the authorised CSP's private key is securely performed under dual control, and that backup copies of the authorised CSP's private key shall be kept in a secure manner;

d) controls over security for the key distribution process including without limitation procedures to ensure the integrity and authenticity of the public key of the authorised CSP which the authorised CSP provides to the Minister for deposit in the CSP disclosure record maintained by the Minister for that authorised CSP;

e) controls over the usage of the key, including the following procedures for activating the key:

more than one responsible officer is required to activate the private key of the authorised CSP; and

the authorised CSP's private key shall only be activated if proper authority for an intended purpose in a prescribed manner is obtained.

f) controls for ensuring that archived keys meet the security and operational requirements stated in the certification practice statement.

5.2 Management process for key generating devices (where appropriate)

5.2.1 An authorised CSP shall maintain an effective management process for key generating devices.

5.2.2 The management process should cover effective procedures and controls over the procurement, receipt, installation, acceptance tests, commissioning, usage, repair, maintenance and retirement of key generating devices, including the following.

a) controls for ensuring the integrity of the cryptographic module;

b) controls for ensuring that the handling of the key generating device is under proper supervision by authorised personnel to prevent the device from being tampered with; and control mechanism established to ensure that the cryptographic modules cannot be tampered with without being detected; and

c) controls for ensuring that the strength of keys generated using cryptographic modules is of an appropriate strength commensurate with the purpose and use of the keys for both the authorised CSP and its subscribers.

5.3 Key management services (where appropriate)

5.3.1 An authorised CSP shall maintain effective procedures and controls over key management services, if any, provided by the authorised CSP to its subscribers, such as key generation, storage, backup, recovery, destruction and archival. Such security procedures and controls shall be consistent with the principles set out in clause 7 of these Guidelines.

5.3.2 An authorised CSP shall ensure there are controls to ensure the safe destruction of key pairs and any related devices including procedures that ensure destruction of all copies of private keys (so that

they cannot be recovered or reconstructed after destruction), revocation of the corresponding public keys and situations where a user asks the CSP to store a copy of a private encryption (not signature) key.

5.4 Key changeover

5.4.1 An authorised CSP shall specify the procedure for the changeover of the authorised CSPs keys and the mechanism for informing the subscribers of the procedure.

5.5 Key compromise and disaster recovery

5.5.1 An authorised CSP shall describe its procedures relating to notification and recovery in the event of key compromise or disaster. It shall address specifically the following:

a) the procedures to recover from situations where its computing resources, software, and/or data are corrupted or compromised, or suspected to be corrupted or compromised; these procedures typically describe how a secure environment is re- established, which accredited certificates are revoked, whether its own key is revoked, how the new CSP public key is provided to the subscribers, and how the subscribers are re-certified;

b) the procedures to recover from a key compromise or suspected key compromise, including the notification of subscribers and relying parties as well as procedures to re- establish its trustworthiness; and

c) the procedures for securing its facility during the period of time following a natural or other disaster and before a secure environment is re-established, either at the original site or a backup site. (An example would be the procedures to protect against theft of sensitive materials from a damaged site).

5.5.2 The Minister must immediately be notified of any of the above events.

6. Management systems and operational guidelines

6.1 Information Security Management System

6.1.1 An authorised CSP shall develop, establish and maintain adequate and proper security control within the context of a management system for its operations based on the generally accepted best security practices given in ISO/IEC 17799 (BS 7799 Part 1) or equivalent and in compliance with Part VIII of the Code of Practice.

Asset Management

6.1.2 An authorised CSP shall maintain an up to date inventory of its major assets, assign an owner who is accountable for each of these assets and establish procedures for protecting these assets.

6.1.3 An authorised CSP shall treat the information that it maintains as one of its assets and protect this information from unauthorised access or damage in accordance with the degree of importance to its business operations, including data that would be within the data protection provisions in the Standard For Electronic Transactions or the scope of data protection regulations made under section 26 of the Act.

Physical security controls

6.1.4 An authorised CSP shall describe the physical controls on its site(s), systems, and equipment in accordance with Chapter 7 of ISO/IEC 17799 (BS 7799 Part 1) or equivalent. Examples of physical security controls include (but not limited to):

a) defining and establishing secure measures for areas housing security sensitive equipment or operations;

b) establishing formal access procedures for staff and for visitors; and

c) establishing appropriate controls to safeguard equipment against unauthorised access as well any potential environmental hazards.

Procedural controls for communications and operations management

6.1.5 Procedural controls and processes are important to ensure the correct and secure operation of the systems and information processing facilities used by an authorised CSP. An authorised CSP shall describe the procedural controls in accordance with Chapters 8 and 10 of ISO/IEC 17799 (BS 7799 Part 1) or equivalent; including (but not limited to):

a) housekeeping tasks such as back-ups and archiving;

b) safeguarding against malicious software;

c) proper handling, distribution, storage and disposal of information and media;

d) handing and resolving operational problems;

e) monitoring system performance and capacity requirements;

f) system maintenance activities; and

g) adequate event logs, which includes the retention of documents for 7 years relating to all major events and incidents and related to the issuing and managing of accredited certificates by the authorised CSP.

Personnel Security

6.1.6 An authorised CSP shall describe the controls it has in place to deal with any personnel security issues in accordance with Chapter 6 of ISO/IEC 17799 (BS 7799 Part 1) or equivalent. This shall include describing its procedural controls for identifying and managing the trusted roles involved in the provision of its certification services. Specific aspects may include:

a) defining specific security roles and responsibilities;

b) incorporating confidentiality or non-disclosure agreements within terms and conditions of employment;

c) providing appropriate training of its personnel with the aim of maintaining competency and ensuring compliance with its security policies and procedures including any retraining period and retraining procedures;

d) maintaining effective procedures for the reporting of security incidents by its staff;

e) recruitment process, including background checks and clearance procedures for personnel filling trusted roles and for those who are engaged in less sensitive positions;

f) performance assessment framework, and disciplinary and termination procedures against personnel for unauthorised actions, improper use of authority, and unauthorised use of systems of the authorised CSP;

g) controls on contractor personnel, including contractual requirements such as indemnification for damages due to the actions of the contractor personnel, monitoring the performance of contractor personnel, etc; and

h) documentation to be supplied to the relevant personnel, such as user manuals, operational procedures, etc, necessary to support these personnel in performing their duties.

System Access

6.1.7 An authorised CSP shall have effective controls and procedures in place to guard against unauthorised access to its information and its systems in accordance with Chapter 9 of ISO/IEC 17799 (BS 7799 Part 1) or equivalent. The controls used for system access shall be appropriate to the sensitivity and criticality of the information and systems being protected, including procedures for (but not limited to):

a) managing user identification and authentication, user access rights and privileges;

b) controlling access to its application systems, networks, operating and mobile systems;

c) guarding against the unauthorised or illegal use of software;

d) monitoring system access and usage; and

e) handling security incidents.

Business Continuity

6.1.8 An authorised CSP shall maintain in accordance with Chapter 11 of ISO/IEC 17799 (BS 7799 Part 1) or equivalent a tried and tested continuity plan to cover contingencies such as recovery of compromise of the certification process, or recovery from major failure of its systems or components of its systems.

Compliance Monitoring

6.1.9 An authorised CSP shall maintain and update in accordance with Chapter 12 of ISO/IEC 17799 (BS 7799 Part 1) or equivalent appropriate controls to ensure compliance with applicable legal and regulatory requirements (as described in section 32 of the Act) and to meet any contractual obligations that apply to its operations.

6.1.10 An authorised CSP shall maintain appropriate controls to ensure that it can monitor compliance with any technical requirements that it is required to satisfy which apply to its operations.

6.1.11 An authorised CSP shall arrange appropriate reviews to be conducted with respect to its operational systems.

6.2 Technical Security Controls

6.2.1 An authorised CSP shall define the general technical security controls it has in place to protect the systems and processes it uses to provide certification services. The authorised CSP shall describe the specific technical security controls used by it to support cryptographic key management and accredited certificate management life cycles.

6.2.2 An authorised CSP should have controls in place to separate the functions and segregate the duties perform by it from those performed by other parties, such as any outsourced functions (e.g. registration function, repositories etc.) and subscribers, so that the responsibilities of the respective parties can be clearly identified.

6.2.3 The security requirements of the CSP outsourcing the management and control of all or some of information systems, networks and/or desk top environments should be addressed in a contract agreed between the parties in accordance with Chapter 4.3 of ISO/IEC 17799 (BS 7799 Part 1) or equivalent.

6.2.4 Specific control areas that may be addressed would include technical controls for the:

a) management of user cryptographic key pairs, including (where appropriate):

   (i) the responsibility for generating the public and private key pair;

   (ii) secure delivery of the private key to subscribers;

   (iii) secure delivery of the subscribers' public key to the accredited certificate issuer;

   (iv) secure delivery of the authorised CSP's public key to subscribers;

   (v) key size adopted, taking into consideration the available technology;

   (vi) controls over generation and quality checking of public key parameters;

   (vii) requirements for the type and quality of cryptographic modules used; and

   (viii) key usage and purpose (e.g. apply key usage flags under the X.509 PKI Certificate Profile version 3 and CRL Profile version 2 standards);

b) private key protection, (*CSP keys)* for example

   (i) the standards, if any, required for the key generation module, such as compliance with a specific level according to the FIPS 140-1 Security Requirements for Cryptographic Modules standard;

   (ii) the use of multi-person control over private keys;

(iii) back up of private keys, including the form of back up and the related security controls of the backup system;

(iv) archive of private keys, including the form of the key archived and the related security controls of the archival system;

(v) controls over the activation, usage and deactivation of the private keys, including for example the number of persons required for key entry, the form of the private keys, the activation mechanism, the active period of an activated key, etc;

(vi) controls over the destruction of the private keys, destruction of tokens, or overwriting keys;

(vii) public key archival; and

(viii) usage period for public and private keys;

c) controls over activation data, which outline the controls over the life cycle of activation data, from generation, distribution, through to archival and destruction. Control considerations should be similar to those for key pair generation and private key protection described above;

d) computer security controls, which outline the security features in place to prevent and detect unauthorised access, modification, or compromise of the systems of the authorised CSP. Reference where appropriate may be made to an appropriate computer security evaluation rating framework, such as ISO 15408:1999 Common Criteria for Information Technology Security Evaluation (CC);

e) system development life cycle controls, which outline the controls implemented by the authorised CSP over the development life cycle of its systems, covering mechanisms and procedures for purchasing or developing the software and hardware for the initial configuration of the equipment of the authorised CSP to prevent tampering;

f) network security controls, which outline the control to protect all connectivity to equipment of the authorised CSP, such as an appropriately configured and maintained firewall, or equivalent access control device,

as well as the monitoring of unauthorised access attempts and prevention against malicious attacks; and

g) engineering controls for cryptographic module. These may be referenced to an appropriate standard, such as FIPS 140-1 Security Requirements for Cryptographic Modules or some equivalent engineering standard.

6.3 Security review procedures

6.3.1 An authorised CSP shall describe event logging and review systems that are implemented by it for the purpose of maintaining a secure environment. Elements include the following:

Types of events recorded

6.3.2 An authorised CSP shall describe the types of events to be recorded. At a minimum. it shall, using operational procedures and audit controls, record:

a) suspicious network activity;

b) repeated failed access attempts;

c) events related to equipment and software installation, modification, and configuration within the entire CSP operation;

d) privileged accesses to all CSP components; and

e) regular accredited certificate management operations, such as:

accredited certificate revocation and suspension requests;

actual issuance, revocation, and suspension of accredited certificates;

accredited certificate renewals;

updates to any repository(ies);

CRL generation and posting;

CSP key rollover;

backups; and

emergency key recoveries.

6.3.3 To the extent practicable, the events recorded shall identify the entities or individuals that triggered the event and include any action taken in response and by whom. All entries shall be dated and time stamped.

6.3.4 It is a good practice for the authorised CSP to first establish the thresholds for severity and significance of individual security-related events and trends based on currently accepted practices. All events and significant trends beyond those thresholds shall be recorded.

6.3.5 An authorised CSP shall implement separation of privilege and other mechanisms or procedures to ensure the integrity of all records. The mechanisms and procedures used to implement separation of privilege shall be described by the authorised CSP.

Frequency of processing event logs

6.3.6 An authorised CSP shall specify the frequency with which the event logs are processed, e.g. consolidated and reviewed.

Retention period for event logs

6.3.7 An authorised CSP shall specify the retention period for event logs, which shall conform to the requirements in this Code of Practice.

Protection of event logs

6.3.8 An authorised CSP shall specify the mechanism in place to protect the event logs from accidental damage or deliberate modifications.

Event log backup procedures

6.3.9 An authorised CSP shall specify the procedures for backing up the event logs, as well as the retention period for the backups. It is a good practice to ensure that the storage facility can afford the backups adequate protection against theft, destruction, or media degradation. Further, it is important to ensure that the method of storage and retrieval of the data must remain current and functional for the life of the archive.

6.4 Records archival

6.4.1 An authorised CSP shall describe its policy relating to general records retention. As a general rule, the authorised CSP shall ensure that archived records are detailed enough to establish the validity of an accredited certificate and the proper operation of it in the past. Typical data that the authorised CSP may consider for archiving could include:

a) data relating to the initialisation of the CSP equipment, such as

   (i) system equipment configuration files;

   (ii) results of assessments and/or reviews for accreditation of the equipment (if conducted);

   (iii) certification practice statement; and

(iv) any contractual agreements to which the authorised CSP is bound; and

b) data relating to the operation of the authorised CSP, such as

(i) modifications or updates to any of the above data items;

(ii) all accredited certificates and CRLs (or other revocation information) as issued or published;

(iii) periodic event logs (see section 5.5); and

(iv) other data necessary for verifying archive contents.

Retention period for archive

6.4.2 An authorised CSP shall archive records for a retention period of 7 years, which shall conform to the requirements in this Code of Practice.

Protection of archive

6.4.3 An authorised CSP shall specify the procedures in place to protect the archived records, covering for example:

a) the custodian of such archives;

b) the mechanism for accessing such records, such as for the purpose of reviews or for the resolution of disputes; and

c) the mechanism for protecting the archive from accidental destruction, deliberate modification, theft, or media degradation.

Archive backup procedures

6.4.4 The authorised CSP shall specify the procedures for backing up the archived records, as well as the retention period of the backups.

Made this day of , 2002

Minister of Telecommunications and E-Commerce