ACCOP Paper No. 3/2003

Splitting of the Assessment of a Certification Authority into Two Parts

Introduction

In respect of the review of the Electronic Transactions Ordinance (ETO) (Cap. 553) conducted in 2002, one of the proposals is to split into two parts the assessment required under the ETO of a certification authority (CA) on its compliance with the provisions of the ETO applicable to CAs and the Code of Practice for Recognized Certification Authorities (Code of Practice). It is proposed that the first part, which concerns provisions related to the trustworthiness of the certification service, should be prepared by a qualified and independent person, and the second part, which concerns provisions not related to the trustworthiness of the certification service, should be dealt with through a declaration by a responsible officer of the CA. This paper sets out a proposed classification of the provisions to be dealt with by the independent assessment and by the self-declaration respectively.

Background

2. Currently, under section 20(3)(b) of the ETO, a CA applying for recognition has to engage an assessor approved by the Director of Information Technology Services (the Director) to prepare an assessment report. The report provides an assessment on the CA's capability to comply with provisions of the ETO applicable to CAs and the Code of Practice. For recognized CAs, such assessment has to be conducted at least once in every 12 months as required under section 43(1) of the ETO, and is also required when recognized CAs apply for renewal of the recognition status under section 27.

3. The provisions of the ETO and Code of Practice relevant to assessment of CAs generally fall into two categories. The first category is related to trustworthiness of the CA operation (e.g. system security, procedural safeguard and financial viability, etc.). The second category is not related to trustworthiness but other aspects of the CA operation, e.g. the requirement to take care of the needs of persons with disabilities in the provision of the CA's services.

4. The Government has committed to review the ETO, which was enacted in January 2000, to ensure that Hong Kong has the most up-to-date legislative framework for the conduct of e-business. The Government conducted a public consultation exercise on a set of preliminary proposals to improve and update the ETO from March to April 2002. In November 2002, the Commerce, Industry and Technology Bureau (CITB) briefed the Legislative Council Panel on Information Technology and Broadcasting on the results of the public consultation and the revised proposals formulated having considered the public comments received.

5. One of the proposals is to amend the ETO to split the assessment of a CA into two parts in order to facilitate the conduct of the assessment. The first part will cover the provisions of the ETO applicable to CAs and the Code of Practice relating to the trustworthiness of the CA operation and has to be handled by an independent and qualified assessor approved by the Director. The second part will cover the provisions of the ETO applicable to CAs and the Code of Practice not relating to the trustworthiness of the CA operation and can be dealt with through a declaration made by a responsible officer of the CA, as defined under section 2 of the ETO.

6. Most respondents to the public consultation on the review of the ETO supported the proposal to split the assessment into two parts. Some respondents considered that there should be clear guidelines on which provisions of the ETO and the Code of Practice are to be assessed by an independent and qualified assessor and which are to be dealt with by self-declaration. The Government agrees that this should be set out clearly to facilitate the conduct of the assessments and proposes to amend the ETO to empower the Director to specify in the Code of Practice those provisions of the ETO applicable to CAs and the Code of Practice that are to be assessed by an independent and qualified assessor and those to be dealt with through a self-declaration.

Classification of provisions of ETO and Code of Practice

7. We have set out at Annex a proposed classification of the provisions of the ETO applicable to CAs and the Code of Practice. Part A covers provisions that are related to the trustworthiness of the CA operation and have to be covered by the assessment to be performed by an independent and qualified assessor approved by the Director. Part B covers provisions relating to other aspects of the CA operation and can be dealt with through a declaration to be made by a responsible officer of the CA.

Advice Sought and Way Forward

8. Members are invited to comment on the proposed classification of the provisions of the ETO applicable to CAs and the Code of Practice as set out at Annex.

9. The Government intends to introduce the proposed legislative amendments into the Legislative Council within the current legislative session. Subject to the passage of the proposed legislative amendments, the Director will finalise the classification of the provisions in the light of Members' comments and publish them in the Code of Practice. Members will be consulted again before the Director finalises the classification.

Information Technology Services Department
January 2003

Annex

Classification of Provisions of ETO and Code of Practice in relation to Assessment of a CA

A. Assessment to be performed by an independent assessor

A.1 Provisions of the ETO within the scope of assessment

Section	Brief description
Part VII : Recognition of CAs and certificates by Director	
21(4)(a)	In determining whether an applicant is suitable for recognition, the Director shall take into account the financial status of the applicant. (See Note 1 below)
21(4)(b)	In determining whether an applicant is suitable for recognition, the Director shall take into account arrangements of the applicant to cover liabilities. (See Note 1 below)
21(4)(c)	In determining whether an applicant is suitable for recognition, the Director shall take into account the system, procedure, security arrangements and standards used by the applicant to issue certificates. (See Note 1 below)
21(4)(f)	In determining whether an applicant is suitable for recognition, the Director shall take into account the reliance limits set by the applicant for its certificates. (See Note 1 below)
Part X : General Provisions as to Recognized CAs	
36	Publication of issued and accepted certificates
37	Recognized CA to use trustworthy system
39	Representations upon issuance of recognized certificate
40	Representations upon publication of recognized certificate
42(1)	Recognized CA not liable for loss caused by reliance on a false or forged digital signature (See Note 2 below)

Section	Brief description
42(2)	Recognized CA not liable in excess of the reliance limit specified in the certificate (See Note 2 below)
44	Recognized CA to issue a certification practice statement
45(1)	Recognized CA to maintain repository
Part XI : Provisions as to secrecy, disclosure and offences	
46	Obligation of secrecy (See Note 3 below)
47	False information (See Note 3 below)
48	Other offences (See Note 3 below)

Note :

1. The assessment shall cover the aspect of CA operation (i.e. financial status, liability cover, etc.) as referred to in the section of the ETO concerned. The Director will take into account the relevant information contained in the assessment report in determining whether an applicant is suitable for recognition.
2. The assessment report shall contain information on whether the CA has waived the application of the section of the ETO concerned, thus increasing the CA's potential liability.
3. The assessment report shall contain information on instances, if any, where the CA has contravened the section of the ETO concerned and which the assessor is aware of in the course of his work.

A.2 Provisions of the Code of Practice within the scope of assessment

Section	Brief description
3. General Responsibilities of a Recognized CA	
3.1	Compliance with conditions of recognition
3.2	Appointment of agents or subcontractors
3.3	Reasonable care in issuing certificates
3.4	To furnish the Director with a copy of CA certificate

Section	Brief description
3.5	Recording, retaining or archiving of information and record
3.6	Privacy of personal information.
3.8	Issuance of both recognized certificates and non-recognized certificates
4. Certification Practice Statement (CPS)	
4.1	Publication of CPS
4.2	Specification of liabilities, rights, obligations and reliance limits in CPS
4.3	Provision of up-to-date information in CPS
4.4	Significance of using and relying upon non-recognized certificates
4.5	Subscribers' personal information to become public information
4.6	Submission of CPS to the Director
4.7	Certificate policy to be considered as part of CPS
4.8	Retention of a copy of each version of CPS
4.9	Compliance with CPS in issuing recognized certificates
4.10	Availability of CPS in on-line and publicly accessible repository
4.11	Standards and procedures of CPS set out in the Appendix
4.12	Consultation with the Director in respect of intended material changes to CPS
4.13	Notification of any incident that adversely and materially affects the validity of the whole or any part of CPS
5. Trustworthy System	
5.1	Use of trustworthy system in performing CA's services
5.2	System to perform its intended functions in a consistent, reliable and dependable manner
5.3	Adequacy of the mechanisms, procedures and conditions under which the CA's system operates
5.6	Adoption of widely accepted standards; performance of assessments to ascertain risks; implementation of counter-measures for managing, mitigating and monitoring risks
5.7	Hardware, software and cryptographic components to be supported by appropriate security policies and procedures
5.8	Adherence to generally accepted good practices
5.9	Establishment and maintenance of policies, procedures and practices over

Section	Brief description
	operational environment
5.9.1	Establishment and maintenance of adequate and proper security control
5.9.1 (a)	Asset classification and management
5.9.1 (b)	Personnel security
5.9.1 (c)	Physical and environmental security
5.9.1 (d)	Management over systems access
5.9.2	Maintenance of effective controls and procedures in respect of day-to-day operation
5.9.3	Development and maintenance of computer systems with effective controls and procedures
5.9.4	Establishment and maintenance of business continuity plan
5.9.5	Testing of continuity plan on a regular basis
5.9.6	Coverage of contingencies by the continuity plan
5.9.7	Maintaining adequate event journals
5.9.8	Archiving of event journals
5.9.9	Maintain journals relating to all major events
5.9.10	Compliance monitoring and assurance
5.10	Establishment and maintenance of policies, procedures and practices over specific functions of a recognized CA
5.10.1	Management of CPS
5.10.2	Monitoring and compliance in respect of legal and regulatory requirements
5.10.3	Management of recognized CA's own keys
5.10.4	Management of key generating devices
5.10.5	Maintenance of procedures and controls over key management services
5.10.6	Management of tokens
5.10.7	Management of certificates
5.10.8	Management of the certificate revocation list
5.11	Provision of trustworthy system to generate keys
5.12	Keeping of recognized CA's own private key and the activation data separately
5.13	Retention of records

Section	Brief description
5.14	Archiving of certificates
5.15	Technical implementation for the creation of a digital signature
5.16	Notification of incidents which materially and adversely affect recognized CA's trustworthy system
5.17	Requirement for personnel to possess necessary knowledge, technical qualifications and expertise
5.19	Adoption of security policy in accordance with generally accepted security principles
5.20	Establishment of security incident reporting and handling procedure, and disaster recovery set-up and procedure
5.21	Implementation of risk management plan
6. Certificates and recognized certificates	
6.1	Use of separate private keys to sign recognized certificates and non-recognized certificates respectively
6.2	Information in certificates to locate CPS
6.3	Issuance of recognized certificate only upon request from applicant and in compliance with practices and procedures set out in CPS
6.4	Reasonable opportunity for subscriber to verify the contents of the recognized certificate before accepting the certificate
6.5	Publication of recognized certificates
6.6	Consent of subscriber to include personal information in the certificate
6.7	Notifying the subscriber of any fact that affects the validity or reliability of the recognized certificate
6.8	Indication of validity period in recognized certificate
6.9	Representation that the recognized certificate has been issued in accordance with CPS
6.10	All transactions related to issuance of recognized certificates shall be recorded.
6.11	Revocation and suspension of recognized certificates
6.12	Information in recognized certificate to locate repository
6.13	Suspension or revocation of recognized certificate within a reasonable time
6.14	Publication of notice of the suspension or revocation of recognized certificate in repository

Section	Brief description
6.15	Agreement in respect of the time of revocation or suspension of certificate as well as the allocation of liability
6.16	Temporary suspension of recognized certificate
6.17	Immediate revocation of recognized certificate
6.18	Checking of whether the recognized certificate to be suspended shall be revoked or reinstated after suspension
6.19	Notification of suspension or revocation of recognized certificate
6.20	Provision of hotline or other reporting facilities
6.21	All transactions in relation to suspension or revocation shall be recorded.
6.22	Recognized certificate subject to renewal upon expiry of its validity
6.23	All transactions in relation to renewal shall be recorded.
7. Verification of subscriber's identity	
7.1	Specification of procedure to verify the identity of applicant
7.2	Retention of documentary evidence for subscriber identification
8. Reliance limit	
8.1	Specification in respect of the significance of reliance limit
8.2	Insurance or other forms to cover liability
9. Repositories	
9.1	To make available on-line and publicly accessible repository
9.2	Not to carry out any activities in a manner that creates unreasonable risks to relying parties
9.3	Information to be contained in repository
9.4	Repository not to contain inaccurate or unreliable information
9.5	Keeping an archive of recognized certificates in repository
10. Disclosure of information	
10.1	Publication of information in repository
10.2	Informing the Director of any changes in the appointment of responsible officers
10.3	Submission of progress reports to the Director at 6-month intervals
10.4	Reporting of changes in the information referred to under section 10.3

Section	Brief description
10.5	Reporting of events leading to potential conflict of interest
10.6	Reporting of incidents that materially and adversely affect the recognized CA's operation
10.7	Granting of licence to the Director for reproduction and publication of reports or information submitted by the recognized CA
10.9	Not to attempt to prevent the Director from publishing any information for the purposes of the Ordinance
11. Termination of service	
11.1	Submission of termination plan
11.2	Termination plan to specify the arrangements for the termination of the recognized CA's service
11.3	Termination scenarios and measures to be covered
11.4	Reference of termination plan in CPS
11.5	Announcement of termination of service, revocation of certificates and transfer of information in repository
12. Assessment of compliance with ETO and Code of Practice	
12.1	Submission of an assessment report at least once in every 12 months
13. Adoption of standards and technology	
13.1	Continuous review and update of standards and technology
14. Inter-operability	
14.1	Adoption of open and common interface to facilitate the verification of digital signature
14.2	Disclosure of open and common interfaces supported and inter-operability arrangements with other CAs.
Appendix	
Entire Appendix	Standards and procedures regarding the contents of certification practice statements

B. Declaration of compliance with ETO and Code of Practice to be made by a responsible officer of certification authority

B.1 Provisions of the ETO to be dealt with by means of declaration

Section	Brief description
Part VII : Recognition of CAs and certificates by Director	
21(4)(e)	In determining whether an applicant is suitable for recognition, the Director shall take into account whether the applicant and the responsible officers are fit and proper persons. (Note 1 : Arising from this section of the ETO, the declaration shall state whether a CA and its responsible officers are fit and proper persons. Note 2 : Under the ETO, whether a person is fit and proper is to be considered having regard to, among other things, whether the person has a conviction or is bankrupt. Currently, each responsible officer of a CA applying for recognition is required to furnish the Director with a declaration to the effect that the responsible officer is a fit and proper person under the meaning of the ETO. Each responsible officer is also required to submit an authorisation for the Commissioner of Police to release criminal convictions recorded against the responsible officer to the Director. With the authorisation, the Director will enquire with the Commissioner of Police whether the responsible officer concerned has been convicted before. The Director will also check with the Official Receiver to see if there is any bankruptcy case against the responsible officer. The Director will continue to adopt the above practices when considering whether a responsible officer of a CA applicant is a fit and proper person.)

B.2 Provisions of the Code of Practice to be dealt with by means of declaration

Sections	Brief description
3. General Responsibilities of a Recognized CA	

Sections	Brief description
3.7	Not to engage in restrictive practices that impair economic efficiency or free trade.
3.9	To take care of the needs of persons with disabilities in the provision of services
5. Trustworthy System	
5.18	Responsible officers and those officers with trusted roles shall be fit and proper persons. (See Notes 1 and 2 in section B.1 above)
15. Consumer protection	
15.1	Advertisement of services shall be decent, honest and truthful.