

The Code of Practice for Recognized Certification Authorities and related Guidance / Information Notes

Introduction

This paper briefs members on the Code of Practice for Recognized Certification Authorities (the Code of Practice) which the Director of Information Technology Services (the Director) has issued under section 33 of the Electronic Transactions Ordinance (Cap. 553) (the Ordinance), and the related guidance / information notes.

Background

2. The Government introduced the Electronic Transactions Bill into the Legislative Council in July 1999 for the establishment of a clear framework conducive to the conduct of electronic transactions. The Bill was passed by the Legislative Council on 5 January 2000 and the Electronic Transactions Ordinance (Cap. 553) was gazetted on 7 January 2000. The Ordinance gives legal recognition to electronic records and digital signatures and provides a framework to promote and facilitate the establishment and operation of recognized certification authorities (CAs).

3. The Government encourages private sector initiatives to provide CA services. In line with our minimalist approach, there is no mandatory licensing requirement under the Ordinance. However, in order to protect consumer interests and enhance public confidence in electronic transactions, the Ordinance provides for a voluntary recognition scheme whereby CAs may apply to Government for recognition on a voluntary basis. Under the Ordinance, the Director is the authority to grant Government recognition to CAs and to the certificates issued by recognized CAs.

The Code of Practice

4. In accordance with section 33 of the Ordinance, the Director has issued the Code of Practice specifying standards and procedures for recognized CAs to carry out their functions.

5. Section 20(3)(b) of the Ordinance states that a CA seeking recognition must furnish to the Director a report which contains an assessment as to whether the CA is capable of complying with the provisions of the Ordinance applicable to a recognized CA and the Code of Practice. The report shall be prepared by a person acceptable to the Director as being qualified to give the report. The Director shall consider, in addition to any other relevant matters, the assessment contained in the report in determining whether the CA is suitable for recognition under the Ordinance.

6. Section 43(1) of the Ordinance states that at least once in every 12 months, a recognized CA must furnish to the Director a report containing an assessment as to whether the recognized CA has complied with the provisions of the Ordinance applicable to a recognized CA and the Code of Practice during the report period. The report must be prepared by a person approved by the Director as being qualified to make such a report. Failure to meet the requirements as set out in the Code of Practice may be a ground for the Director to suspend or revoke the recognition granted to a recognized CA or to reject the application by a recognized CA for renewal of its recognition.

7. Qualifications of the person to prepare the assessment report of a CA are set out in section 12 of the Code of Practice.

8. Section 37 of the Ordinance states that a recognized CA must use a trustworthy system in performing its services. Detailed guidelines for the implementation of a trustworthy system are provided in section 5 of the Code of Practice.

9. There is an appendix to the Code of Practice which sets out the standards and procedures regarding the contents of a certification practice statement (CPS). These standards and procedures are based on the

"Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework" published by the Internet Engineering Task Force (commonly referred to as IETF PKIX Part 4). Recognized CAs are expected to adopt and to comply with these standards and procedures when issuing their CPSs.

Related Guidance/information Notes

10. Together with the Code of Practice, the Director has also issued the following guidance and information notes -

- Guidance Note on Recognition of Certification Authorities and Certificates which outlines the conditions and the process for the recognition of CAs and certificates;
- Guidance Note on Compliance Assessment of Certification Authorities which provides guidance on the scope and conduct of the assessment required under section 20(3)(b) or section 43(1) of the Ordinance in respect of a CA intending to seek recognition or a CA already recognized as the case may be;
- Guidance Note on the Procedures of Appeal against Decisions of the Director of Information Technology Services in respect of the Director's refusal of an application for recognition or for renewal of a recognition, or in respect of the Director's decision to revoke or suspend a recognition under the Ordinance; and
- Information Note on the Advisory Committee on Code of Practice for Recognized Certification Authorities which sets out the terms of reference and membership of the Advisory Committee.

Public Consultation

11. The Director may from time to time amend the Code of Practice. The Director may consult the industry, including CAs recognized under

sections 21 and 34 of the Ordinance, in respect of amendments to the Code of Practice. The primary channel of consultation with the industry will be through the Advisory Committee on Code of Practice for Recognized Certification Authorities.

Information Technology Services Department
January 2000