



# **Digi-Sign Certification Services Limited**

---

## **Certification Practice Statement**

(OID: 1.3.6.1.4.1.8420.1.1.11)

**In support of Digi-Sign CA as a Recognised Certification Authority**

**July 2003**

# Table of Contents

<b>1.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
1.1	GENERAL DESCRIPTION.....	1
1.2	CONTACT DETAILS .....	2
<b>2.</b>	<b>CLASSES OF CERTIFICATES &amp; KEY ATTRIBUTES .....</b>	<b>4</b>
2.1	CLASSES OF ID-CERT .....	4
2.2	ACCREDITED ORGANIZATION .....	6
2.3	IDENTIFICATION.....	7
2.4	COMMUNITY & APPLICABILITY.....	8
2.5	SCOPE OF USAGE OF ID-CERT.....	9
2.6	LIFE CYCLE OF ID-CERT .....	10
<b>3.</b>	<b>GENERAL PROVISIONS.....</b>	<b>11</b>
3.1	OBLIGATIONS.....	11
3.1.1	<i>Certification Authority Obligations and Duties</i> .....	13
3.1.2	<i>Subscriber Obligations and Duties</i> .....	13
3.1.3	<i>Relying Party Obligations and Duties</i> .....	14
3.1.4	<i>Repository Obligations and Duties</i> .....	14
3.2	LIABILITIES .....	15
3.2.1	<i>Disclaimers &amp; Limitations on Warranties</i> .....	16
3.2.2	<i>Time Limitation</i> .....	16
3.2.3	<i>Other Exclusions</i> .....	16
3.4	FINANCIAL RESPONSIBILITY.....	17
3.5	INTERPRETATION & ENFORCEMENT .....	17
3.5.1	<i>Governing Law</i> .....	17
3.5.2	<i>Severability</i> .....	17
3.5.3	<i>Survival</i> .....	17
3.5.4	<i>Notice</i> .....	17
3.5.5	<i>Agreement</i> .....	18
3.5.6	<i>Dispute Resolution</i> .....	18
3.6	FEES.....	18
3.7	PUBLICATION & REPOSITORY.....	18
3.8	COMPLIANCE ASSESSMENT.....	19
3.9	CONFIDENTIALITY POLICY.....	19
3.10	INTELLECTUAL PROPERTY RIGHTS .....	19
<b>4.</b>	<b>IDENTIFICATION AND AUTHENTICATION.....</b>	<b>20</b>
4.1	INITIAL CERTIFICATION.....	20
4.1.1	<i>Types of Names</i> .....	22
4.1.2	<i>Need for Meaningful Name</i> .....	23
4.1.3	<i>Rules for Interpreting Various Name Formats</i> .....	24
4.1.4	<i>Uniqueness of Names</i> .....	25
4.1.5	<i>Name Dispute Resolution Procedures</i> .....	25
4.1.6	<i>Verification of Subscriber Identity</i> .....	25
4.1.7	<i>Method of Proof of Possession of Private Key</i> .....	26
4.1.8	<i>Online Applications</i> .....	26
4.2	CERTIFICATE RENEWAL.....	26
4.3	APPLICATION AFTER REVOCATION .....	27
4.4	REVOCATION REQUEST .....	28
4.5	SUSPENSION REQUEST .....	29
<b>5.</b>	<b>OPERATIONAL REQUIREMENTS .....</b>	<b>31</b>
5.1	SUBSCRIBER APPLICATION.....	31
5.2	CERTIFICATE ISSUANCE.....	31
5.2.1	<i>Key Generation</i> .....	31
5.2.2	<i>Delivery of Keys</i> .....	31



5.3	CERTIFICATE ACCEPTANCE.....	32
5.3.1	<i>Responsibility of Subscriber</i> .....	32
5.3.2	<i>Notification of Change</i> .....	32
5.4	CERTIFICATE SUSPENSION & REVOCATION.....	32
5.4.1	<i>Certificate Suspension</i> .....	32
5.4.2	<i>Updating of the CRL</i> .....	32
5.5	SECURITY REVIEW PROCEDURES .....	32
5.5.1	<i>Event Logging</i> .....	33
5.5.2	<i>Frequency of Processing Log</i> .....	33
5.5.3	<i>Retention Period for Processing Log</i> .....	33
5.5.4	<i>Protection of Processing Log</i> .....	33
5.5.5	<i>Backup of Processing Log</i> .....	33
5.6	INFORMATION AND RECORD ARCHIVAL.....	34
5.6.1	<i>Retention Period</i> .....	34
5.6.2	<i>Protection of Archive</i> .....	34
5.6.3	<i>Archive Backup Procedures</i> .....	34
5.7	KEY CHANGEOVER .....	34
5.8	CA KEY MANAGEMENT.....	35
5.9	KEY COMPROMISE AND DISASTER RECOVERY.....	35
5.10	TERMINATION OF CA OPERATIONS.....	35
<b>6.</b>	<b>PHYSICAL, PROCEDURAL &amp; PERSONNEL SECURITY CONTROLS .....</b>	<b>36</b>
6.1	PHYSICAL SECURITY.....	36
6.2	PROCEDURAL CONTROLS .....	37
6.3	PERSONNEL SECURITY CONTROLS.....	37
<b>7.</b>	<b>TECHNICAL SECURITY CONTROLS.....</b>	<b>39</b>
7.1	KEY PAIR GENERATION AND INSTALLATION.....	39
7.2	DIGI-SIGN CA PRIVATE KEYS PROTECTION .....	40
7.3	ACTIVATION DATA .....	41
7.4	COMPUTER SECURITY CONTROLS.....	41
7.5	PUBLIC KEY ARCHIVAL.....	41
7.6	SYSTEM DEVELOPMENT LIFE CYCLE CONTROLS.....	41
7.7	NETWORK SECURITY CONTROLS .....	42
7.8	CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS .....	42
<b>8.</b>	<b>CERTIFICATE AND CRL PROFILES.....</b>	<b>43</b>
8.1	CERTIFICATE PROFILE .....	43
8.2	CRL PROFILE.....	43
<b>9.</b>	<b>CPS ADMINISTRATION.....</b>	<b>44</b>
<b>10.</b>	<b>INTEROPERABILITY.....</b>	<b>46</b>
<b>11.</b>	<b>GLOSSARY OF TERMS.....</b>	<b>47</b>

## Appendices:

- 1 Digi-Sign Certification Services Limited ID-Cert Profile
  - Personal ID-Cert Class 1 Certificate Specification
  - Organizational ID-Cert Class 2 Certificate Specification
  - Encipherment ID-Cert Class 3 Certificate Specification
2. Digi-Sign Certification Services Limited ID-Cert CRL Specification



### 3. Digi-Sign Certification Services Limited Key and Certificate Life Cycle Management Plan



## 1. INTRODUCTION

This Certification Practice Statement (“CPS”) is published by Digi-Sign Certification Services Limited (“Digi-Sign”). It sets out:

- ❑ The standards for the provision of the Digi-Sign certification services; and
- ❑ The practices that Digi-Sign employs to enroll Subscribers, verify the Subscriber Applications, manage and control the processing of certificate issuance, acceptance, suspension and revocation.

Digi-Sign is responsible for the preparation of this CPS. Digi-Sign has been assigned the Private Enterprise Number 8420 by Internet Assigned Numbers Authority (IANA). For identification purpose, this CPS bears the Object Identifier (“OID”): 1.3.6.1.4.1.8420.1.1.11.

Digi-Sign will further maintain this CPS to:

- ❑ Show the standards and practices which may be updated from time to time, and
- ❑ Comply with Hong Kong’s *Electronic Transactions Ordinance (Cap. 553)* and *Code of Practice for Recognized Certification Authorities*.

Section 11 herein includes a Glossary of Terms used in this CPS. Digi-Sign reserves its absolute right to revise or interpret this CPS without notice. No agent, employee, or subcontractor of Digi-Sign has the authority to make any representations on behalf of Digi-Sign as to the meaning or interpretation of this CPS without due authorization.

### 1.1 General Description

The structure of this CPS follows the Code of Practice issued by the Director of Information Technology Services. Major headings are as follow:

- ❑ Introduction
- ❑ Classes of Certificates and Key Attributes
- ❑ General Provisions
- ❑ Identification and Authentication
- ❑ Operational Requirements
- ❑ Physical, Procedural, and Personnel Security Controls
- ❑ Technical Security Controls
- ❑ Certificate and CRL Profiles
- ❑ CPS Administration
- ❑ Interoperability

The product name of the certificates issued by Digi-Sign is called “ID-Cert”. There are Personal ID-Cert Class 1, Organizational ID-Cert Class 2 and Encipherment ID-Cert Class 3 issued by Digi-Sign. Issuance of ID-Cert by Digi-Sign is upon its approval of a Subscriber Application, and confirmation of acceptance of the ID-Cert by the person named in the Personal ID-Cert Class 1, or in the case of an Organizational ID-Cert Class 2, by an Authorized Delegate of the organization named therein.



A Personal ID-Cert Class 1 Subscriber or Organizational ID-Cert Class 2 Subscriber may choose to:

- ❑ Apply for an Encipherment ID-Cert Class 3 at the same time as the application for the Personal ID-Cert Class 1 or Organizational ID-Cert Class 2; or
- ❑ Lodge an application for the Encipherment ID-Cert Class 3 subsequently.

Section 2 herein provides further description of the classes of ID-Cert.

A set of rules is stated herein to govern the issuance of ID-Cert. This set of rules also provides the applicability of an ID-Cert to a particular community and / or class of application with common security requirements. These rules may provide a useful means for the users and prospective users of an ID-Cert to determine whether it is sufficiently trustworthy for a particular use, or reliance for a specific purpose. It is the responsibility of a user of the ID-Cert to decide whether to make use of an ID-Cert issued by Digi-Sign to:

- ❑ Authenticate the identity of the person named therein, in the case of a Personal ID-Cert Class 1;
- ❑ Authenticate the identity of the organization named therein, in the case of an Organizational ID-Cert Class 2; or
- ❑ In the case of an Encipherment ID-Cert Class 3:
  - Send encrypted electronic messages to the Subscriber;
  - Decrypt encrypted electronic messages as they are received by the Subscriber; and
  - Issue acknowledgment by the Subscriber upon the receipt of the encrypted electronic message.

This CPS shall not be treated or deemed to be any offer to the Public or any part thereof. Digi-Sign reserves its absolute right to refuse any Subscriber Application, or issue of ID-Cert pursuant to this CPS, without giving any reasons.

## 1.2 Contact Details

For further information about the Digi-Sign certification services or this CPS, the contact details are:

Digi-Sign Certification Services Limited  
Suite 20, 5/F Hong Kong International Trade & Exhibition Centre  
1 Trademart Drive  
Kowloon Bay  
Hong Kong

Digi-Sign Hotline:

Tel: (852) 2917 8833

Fax: 2174 0019

Email: [hotline@dg-sign.com](mailto:hotline@dg-sign.com)

Website: [http:// www.dg-sign.com](http://www.dg-sign.com)

Repository: <ldap.dg-sign.com>



Digi-Sign Certification Practice Statement

Office Hours: Monday to Friday 8:30am to 5:30pm  
Saturday 8:30am to 12:30pm

Emergency Telephone No.: (852) 2917 8833, for use:

- Outside Office Hours;
- On Sunday, or Public Holidays;
- When tropical cyclone warning signal No. 8 or above is hoisted;
- When the “black” rainstorm warning signal is hoisted.



## 2. CLASSES OF CERTIFICATES & KEY ATTRIBUTES

The key attributes indicate the type, class and description of the ID-Cert. Digi-Sign is responsible for defining the scope of recognition, and providing a general description of what such recognition means to Subscribers and relying parties.

### 2.1 Classes of ID-Cert

There are three classes of ID-Cert issued by Digi-Sign under this CPS, namely, the Personal ID-Cert Class 1, Organizational ID-Cert Class 2 and Encipherment ID-Cert Class 3. Description of the ID-Cert is as follows:

#### (1) Personal ID-Cert Class 1

This ID-Cert is issued to individuals to support digital signatures that purport to confirm the identities or other significant characteristics<sup>1</sup> of the individuals who hold a particular key. It is issued to individuals who have attained the age of 18 years and who provide the necessary personal particulars requested by Digi-Sign as per the Subscriber Application form. Such particulars will be checked against the information contained in one of the following documents for verification of the personal identity:

- (a) Hong Kong permanent identity card;
- (b) Hong Kong identity card;
- (c) Valid travel document indicating that the holder's limit of stay in Hong Kong has not expired.

Alternatively, the personal particulars as requested by Digi-Sign according to the Subscriber Application form may be made available to Digi-Sign through an Accredited Organization following the authorization of individuals concerned. Refer to section 2.2 below about Accredited Organization.

#### (2) Organizational ID-Cert Class 2

This ID-Cert is issued to organizations to support digital signatures that purport to confirm the identities or other significant characteristics<sup>2</sup> of the Authorized Delegates who hold a particular key and have been duly authorized to make digital signatures for and on behalf of the organizations. It is issued to organizations which provide the necessary organizational details requested by Digi-Sign as per the Subscriber Application form, including in particular, the following:

- (a) Business registration, or exemption from business registration, under the Business Registration Ordinance (Cap. 310);
- (b) Registration of a company incorporated in Hong Kong Special Administrative Region ("HKSAR"), or registration of an overseas company, under Part XI of the Companies Ordinance (Cap. 32);

---

<sup>1</sup> For details regarding the other significant characteristics, please refer to Subject Alternative Name of the Certification Specification of Personal ID-Cert Class 1 in Appendix 1.

<sup>2</sup> For details regarding the other significant characteristics, please refer to Subject Alternative Name of the Certification Specification of Organizational ID-Cert Class 2 in Appendix 1



- (c) For organizations other than those registered with the Company Registry or Inland Revenue Department of the Government of HKSAR:
  - i. documentation issued by the appropriate registration agency of the Government of HKSAR attesting to the existence of the organization;
  - ii. reference to the relevant legislation for the formation and existence of the organization; and / or
  - iii. written legal opinion given by a legal practitioner practicing the laws of the jurisdiction in which the organization was incorporated on the legal status, capacity, power, formality requirement of and/or restrictions in respect of the use of digital certificate by the organization;
- (d) For bureaux, departments and agencies of the Government of HKSAR, an authorization letter.

Alternatively, the details required by Digi-Sign as per the Subscriber Application form may be made available to Digi-sign through an Accredited Organization following the authorization of the organizations concerned. Refer to section 2.2 below about Accredited Organization.

The Subscriber Application details from the Accredited Organization must include proof of the identity of the applicant organization. Such proof must be adequate in substantiation of the respective Subscriber Application details in (2) (a), (b) and / or (c) above.

For further explanation of (2) above, an applicant organization includes an unincorporated company and a company incorporated in the HKSAR, an overseas company registered in the HKSAR, a statutory body, or an organization that is established under one of the Hong Kong Ordinances.

Applicants for Organizational ID-Cert Class 2 are required to state the personal particulars of an Authorized Delegate. Such personal particulars will be checked against the information contained in one of the documents listed in (1) for Personal ID-Cert Class 1 for verification of the personal identity of the Authorized Delegate. If the nominated Authorized Delegate is already an existing Personal ID-Cert Class 1 Subscriber, this verification will be dispensed with.

### (3) Encipherment ID-Cert Class 3

This ID-Cert is issued to individuals and organizations for encryption and decryption of electronic messages and to support digital signatures (for the issue of acknowledgments by the Subscriber upon receipt of encrypted messages) that purport to confirm the identities or other significant characteristics<sup>3</sup> of the individuals who hold a particular key or Authorized Delegates who hold a particular key and have been duly authorized to make the digital signatures for and on behalf of the organizations. The normal practice is for the Subscriber to lodge a Subscriber Application for the Encipherment ID-Cert Class 3 at the same time as the application for Personal ID-Cert Class 1 or Organizational ID-Cert Class 2, as the case may be.

---

<sup>3</sup> For details regarding the other significant characteristics, please refer to Subject Alternative Name of the Certification Specification of Encipherment ID-Cert Class 3 in Appendix 1



Where the Subscriber Application is submitted separately for the Encipherment ID-Cert Class 3, the applicant must be an existing Personal ID-Cert Class 1 holder, or an existing Organizational ID-Cert Class 2 holder at the time of application for the Encipherment ID-Cert Class 3.

The procedures, controls and relevant requirements for an applicant to lodge an application of an Encipherment ID-Cert Class 3, as well as for Digi-Sign to process the application, will be the same as those for the application for a Personal ID-Cert Class 1 or an Organizational ID-Cert Class 2, as the case may be.

## **2.2 Accredited Organization**

Digi-Sign is responsible to establish the criteria for accreditation of organizations for the purpose of transfer of Subscriber Application details information direct from such organizations in support of Subscriber Applications for ID-Cert. Prior to accreditation, Digi-Sign will verify the following:

- a. The organization providing the Subscriber Application details is a statutory body, or a public body, or is otherwise established under the Hong Kong laws;
- b. The organization has the capability and procedure in place to retain personal identity for the purpose of substantiating the identification of the person applying for Personal ID-Cert Class 1;
- c. The organization has the capability and procedure in place to retain the Subscriber Application details for the purpose of substantiating the identity of the organization applying for Organizational ID-Cert Class 2;
- d. The organization has its privacy policy in conformance to the Personal Data (Privacy) Ordinance (Cap. 486);
- e. For Personal ID-Cert Class 1, the organization providing the Subscriber Application details is in a position to:
  - Demonstrate the procedure to verify the personal identity, such as by “face to face” authentication, or by another method determined by Digi-Sign to be equally effective in authenticating the identity of the applicant;
  - Produce a photocopy of the personal identity, or attest the personal identity, whenever requested by Digi-Sign to do so; and
  - Produce written procedures to show how the personal identity is being kept up-to-date.
- f. For Organizational ID-Cert Class 2, the organization providing the Subscriber Application details is in a position to:
  - Produce photocopies of documentation necessary for identification of an Authorized Delegate and the corresponding organizational identity, or attest the identity of an Authorized Delegate and the corresponding organizational identity, whenever requested by Digi-Sign to do so; and
  - Produce written procedures to show how the Subscriber Application details are being kept up-to-date.
- g. Where the Subscriber’s personal details have been received from an Accredited Organization, the hand-over of the PIN Mailer may be done through the Accredited Organization as a Digi-Sign agent, provided that Digi-Sign is satisfied that the systems



and procedures, including management controls, relevant to the handling of PIN Mailers by the Accredited Organization, are documented and that they are at least as effective and secure as those employed by Digi-Sign. The Accredited Organization will also be subjected to spot checks by Digi-Sign to ensure that the systems and procedures agreed and documented are complied with by the Accredited Organization.

- h. When an organization ceases to be Digi-Sign's Accredited Organization:
  - Digi-Sign will cease accepting Subscriber Application details transferred from this organization.
  - Where the organization also distributes disks and PIN mailers, Digi-Sign will recover any disks and PIN mailers yet to be distributed by the organization and notify the Subscribers that Digi-Sign will distribute the disks and PIN mailers instead.

### **2.3 Identification**

Each ID-Cert bears the OID of this CPS. Full text of this CPS is displayed for public information on the Digi-Sign Website <[www.dg-sign.com](http://www.dg-sign.com)>, and it is accessible online by the Subscribers, and others who may be interested in the information. Digi-Sign reserves its absolute right to, from time to time, change or cancel any existing means of access, and provide other means of access to this CPS.

Digi-Sign undertakes the role of a Recognized Certification Authority under the Electronic Transactions Ordinance (Cap. 553). For this purpose, Digi-Sign has put in place an organizational structure for conducting the various functions. These functions cover the Subscriber registration, trustworthy system operation, communication with the Subscribers and other users, and publication of information. All these functions are under the control of Digi-Sign, although some of the routine tasks in the operation of the trustworthy system are undertaken by Tradelink Electronic Commerce Limited, which wholly owns Digi-Sign, and this is covered by a Service Agreement between the two companies. In addition, Digi-Sign engages the service of a third party to provide facility management of the computer equipment, but retains control of the operation and maintenance of such equipment.

When an Accredited Organization is authorized by Digi-Sign to hand-over PIN Mailers to the Subscribers, such Accredited Organization does so as the agent of Digi-Sign. Digi-Sign shall remain responsible for the operations of agents and subcontractors in so far as the operations are in relation to Digi-Sign as a Recognized Certification Authority. Digi-Sign will also ensure their compliance with the Electronic Transactions Ordinance (Cap. 553) and Code of Practice, while carrying out the operations on behalf of Digi-Sign as a Recognized Certification Authority.

Digi-Sign is responsible for all these functions, and in undertaking this responsibility, Digi-Sign may subcontract some of these functions or part thereof. But no agent, employee, or subcontractor of Digi-Sign has the authority to carry out any acts on behalf of Digi-Sign, except when there is an express delegation of such authority in writing.

ID-Cert Subscribers are registered by Digi-Sign. Each Subscriber is required to enter an agreement (as stated in the terms and conditions specified in the Subscriber Application form) with Digi-Sign. Under this agreement, Digi-Sign and the Subscriber agree that, amongst other things, variation or amendment may be made to this CPS.



In the event of any conflict between this CPS, the terms and conditions specified in the Subscriber Application form, and other rules and guidelines, the terms and conditions specified in the Subscriber Application form shall prevail.

## 2.4 Community & Applicability

Upon issuance of an ID-Cert, Digi-Sign represents to the ID-Cert users that Digi-Sign has carried out the procedures under this CPS in issuing the ID-Cert:

- ❑ In the case of a Personal ID-Cert Class 1, the holder is an individual whose personal particulars are substantiated in the Subscriber Application processed by Digi-Sign in accordance with this CPS;
- ❑ In the case of an Organizational ID-Cert Class 2, the holder is an organization the particulars of which are substantiated in the Subscriber Application processed by Digi-Sign in accordance with this CPS; and
- ❑ In the case of an Encipherment ID-Cert Class 3, the holder is the person or organization whose identity is substantiated in the Subscriber Application processed by Digi-Sign in accordance with this CPS, and holds a Personal ID-Cert Class 1 or an Organizational ID-Cert Class 2.

Upon signing the Subscriber Application form, the Subscriber agrees that he has read the corresponding terms and conditions and to be bound by these terms and conditions during the operational period of the ID-Cert including, but not limited to, the following:

- ❑ In the cases of the Personal ID-Cert Class 1 and Organizational ID-Cert Class 2, the Subscriber must ensure that no other person shall have access to the Subscriber's private key;
- ❑ In the case of the Encipherment ID-Cert Class 3, the Subscriber must ensure that no person other than the Subscriber himself / herself, or upon authorization by the Subscriber, the person(s) delegated the authority to use the certificate, shall have access to the Subscriber's Encipherment ID-Cert Class 3.
- ❑ The Subscribers of Personal ID-Cert Class 1 or Organizational ID-Cert Class 2 warrant that:
  - the personal or organizational information published in the ID-Cert is true and correct at all times;
  - on each occasion a digital signature is generated upon the use of the Subscriber's private key, which corresponds to the public key in the Subscriber's ID-Cert, this digital signature is that of the Subscriber;
  - the ID-Cert is used solely for lawful and legitimate purposes.
- ❑ Subscribers of Encipherment ID-Cert Class 3 shall acknowledge that the digital signature generated by this class of ID-Cert must be used only for the purpose of acknowledging receipt of electronic messages in transactions.
- ❑ Subscribers of Encipherment ID-Cert Class 3 also undertake to restrict the use of the Encipherment ID-Cert Class 3 as described above, and in doing so, it is the duty of the Subscribers to supervise the use of their Encipherment ID-Cert Class 3 by person(s) delegated the authority to use the ID-Cert to use it for the specified purpose only.
- ❑ In the event that the Subscriber makes or delegates the use of the digital signature generated by the Encipherment ID-Cert Class 3 for any purposes other than



acknowledgment of receipt of electronic messages as described herein, the digital signature in such case must be treated as a signature generated and used without the Subscriber's authority, and must be treated for all purposes as an unauthorized signature.

The person who makes use of an ID-Cert, or agrees to rely on an ID-Cert is referred to in this CPS as the relying party.

The relying party has a duty to verify if an ID-Cert is suitable to be relied upon in any particular transaction. The relying party has also a duty to take all necessary steps to ensure that the Subscriber of an ID-Cert has the requisite power and capacity to enter into any particular transaction and all formalities required for execution by the Subscriber in any particular transaction have been complied with. Digi-Sign assumes no duty and will not verify the power and capacity of the Subscriber to enter into any transaction.

## 2.5 Scope of Usage of ID-Cert

Refer to section 2.1 for description of the three classes of ID-Cert issued by Digi-Sign under this CPS. The class of ID-Cert is characterized by the following:

### Personal ID-Cert Class 1

- The applicant in the Subscriber Application is an individual.

### Organizational ID-Cert Class 2

- The applicant in the Subscriber Application is an organization, which may be an unincorporated company, an incorporated company, a statutory body, or a public body scheduled by law, or a bureau, department and agency of the Government of the HKSAR.

### Encipherment ID-Cert Class 3

- The applicant in the Subscriber Application is already an existing holder of Personal ID-Cert Class 1 or Organizational ID-Cert Class 2.

The information relating to each class of ID-Cert, its usage, restriction and prohibition on the usage, is summarized below:

<b>Description of ID-Cert:</b>			
<b>Class</b>	Personal ID-Cert Class 1	Organizational ID-Cert Class 2	Encipherment ID-Cert Class 3
<b>Type</b>	Recognized certificates	Recognized certificates	Recognized certificates
<b>Subscriber</b>	Individuals who have attained the age of 18 years	Companies, organizations, statutory bodies, bureaux, departments or agencies of Government of HKSAR	Individuals who have attained the age of 18 years, companies, organizations, statutory bodies, bureaux, departments or agencies of Government of HKSAR
<b>Liability Cap</b>	Refer to section 3.2 herein	Refer to section 3.2 herein	Refer to section 3.2 herein



<b>Reliance Limit</b>	Refer to section 3.3 herein	Refer to section 3.3 herein	Refer to section 3.3 herein
<b>Limitations:</b>			
<b>Usage of certificate</b>	<input type="checkbox"/> Bind digital signature to electronic mail, electronic transactions and documents, lodgment of compliance information; <input type="checkbox"/> Provide a means of proof of identity for a specific purpose.		<input type="checkbox"/> Encryption & decryption of electronic messages; <input type="checkbox"/> Acknowledgment of receipt of electronic messages.
<b>Restrictions on the usage</b>	Subject to the terms and conditions of this CPS and the Subscriber Application form		
<b>Prohibitions on the usage</b>	Not to be used for illegal or illegitimate purposes, or any other purposes which may be against the law, or by any person or organization other than the Subscriber		

For the information of the Subscribers and relying parties, the above-recognized certificates relate to the classes of recognized certificates issued by Digi-Sign as a Recognized Certification Authority in accordance with the provisions of the Electronic Transactions Ordinance (Cap. 553).

## 2.6 Life Cycle of ID-Cert

An ID-Cert issued in accordance with this CPS has a two-year life cycle, commencing from issuance through to expiry. This two-year life cycle may terminate prematurely upon revocation of the ID-Cert prior to its expiry date, and such revocation is processed according to this CPS.



### 3. GENERAL PROVISIONS

Digi-Sign pledges its commitment to obligations, liability, financial responsibility, and statement of operations covering, amongst others, the governing law, dispute resolution procedures, compliance assessment, and protection of confidentiality.

#### 3.1 Obligations

Digi-Sign recognizes that in its role as a Recognized Certification Authority, it undertakes the responsibility to verify, amongst others:

- The identity of the Subscriber, in the case of a Personal ID-Cert Class 1;
- The identity of the Subscriber, company resolution or similar authorization for the Subscriber Application, in the case of an Organizational ID-Cert Class 2;
- In the case of an Encipherment ID-Cert Class 3 –
  - The identity of the Subscriber if the Subscriber is also a holder of a Personal ID-Cert Class 1;
  - The identity of the Subscriber, company resolution or similar authorization for the Subscriber Application if the Subscriber is also a holder of an Organizational ID-Cert Class 2.

Digi-Sign assumes no duty and will not verify the power and capacity of the Subscriber to enter into any transaction.

The above role is to be carried out in accordance with this CPS. Digi-Sign also sets specific obligations upon its Subscribers, and the relying parties of the ID-Cert. At the date of this CPS, Digi-Sign has entered no agreement or arrangement with another certification authority for cross certification. But Digi-Sign reserves its absolute right to do so at a later stage.

Digi-Sign's obligations and duties are defined by the terms and conditions associated with the Subscriber Application form and this CPS. All relying parties of the ID-Cert must note that Digi-Sign is committed only to reasonable care and skill in performing its certification services under this CPS.

Digi-Sign is not an agent, trustee, or other representative of its Subscribers, or of the relying party of the ID-Cert, and undertakes no fiduciary responsibility towards its Subscribers, or the relying parties at any time. Save and except expressly provided in this CPS and the terms and conditions specified in the Subscriber Application form, the Subscribers and relying parties do not have the authority to bind Digi-Sign by contract or otherwise to any obligation.

Digi-Sign is responsible for providing its services under the terms and conditions specified in the Subscriber Application form and this CPS. In doing so, there is no sale of goods by Digi-Sign. The ID-Cert, information published, and any materials or software delivered to the Subscribers, or other users, shall remain the property of Digi-Sign.

Digi-Sign further declares that there are no express or implied terms, and there is no warranty as to the fitness for use for a particular purpose, relevant to an agreement for the supply of goods, other materials or software provided to the Subscribers, or information published. A Subscriber's right, and that of any other persons, is restricted to the use of the ID-Cert, such



## Digi-Sign Certification Practice Statement

information, materials, or software under the terms and conditions specified in the Subscriber Application form and this CPS.



### **3.1.1 Certification Authority Obligations and Duties**

As a Recognized Certification Authority under the Electronic Transactions Ordinance (Cap. 553), Digi-Sign undertakes to meet its obligations and carry out its duties as defined by the terms and conditions specified in the Subscriber Application form and this CPS.

In summary, Digi-Sign is committed to performing its certification services and operations substantially according to this CPS, encompassing, but not limited to, the following:

- ❑ Comply with the Electronic Transactions Ordinance (Cap 553) and Code of Practice, and carry out the responsibilities and duties specified therein;
- ❑ Publish this CPS in a manner that the information is readily accessible;
- ❑ Maintain the life cycle and protect the security of the Digi-Sign CA keys;
- ❑ Notify the Subscriber of the issuance of ID-Cert, including the timing of its issuance;
- ❑ Issue the private key and ID-Cert to the Subscriber;
- ❑ Protect the security of the private key before and during its delivery to the Subscriber;
- ❑ Publish the list of ID-Cert and list of Subscribers;
- ❑ Publish a list of the ID-Cert suspended or revoked, and notify the Subscriber of the suspension or revocation, including the timing of such suspension or revocation.

### **3.1.2 Subscriber Obligations and Duties**

Digi-Sign requires each Subscriber to enter an agreement (as stated in the terms and conditions specified in the Subscriber Application form), which amongst other things, binds a Subscriber to obligations encompassing, but not limited to, the following:

- ❑ Read and understand this CPS before using the ID-Cert and the private key;
- ❑ Use the ID-Cert and the private key strictly in accordance with the terms and conditions specified in the Subscriber Application form and this CPS;
- ❑ Provide true and correct information to Digi-Sign upon applying to Digi-Sign for the ID-Cert, and notify Digi-Sign immediately of any changes thereafter;
- ❑ Notify Digi-Sign immediately upon the occurrence of the following:
  - Loss of the private key
  - Compromise or suspected compromise of the private key
  - Failure of the protection of the private key, or suspected failure of the protection
- ❑ Notify the relying party of the above occurrences, where the ID-Cert has been used in any transaction or communication from the Subscriber to the relying party;
- ❑ Undertake to stop the use of the ID-Cert immediately upon the following:
  - The Subscriber has lodged a request with Digi-Sign to revoke the ID-Cert, or has been notified by Digi-Sign of the revocation of the ID-Cert under this CPS
  - The Subscriber has become aware of any event that Digi-Sign would normally rely upon as reason for revocation of the ID-Cert, as listed in section 4.4 (a) herein
- ❑ Undertake not to:



- Use the private key in a manner that may infringe the rights of a third party;
- Assign any rights under the terms and conditions specified in the Subscriber Application form.
- Indemnify Digi-Sign against any direct and indirect costs incurred by Digi-Sign as a result of the Subscriber's:
  - failure to maintain the protection of the private key; or
  - misuse of the private key
- Undertake to carry out the Subscriber's duty and responsibility, and that upon any failure to do so, the Subscriber is bound by the terms and conditions specified in the Subscriber Application form in terms of liability to Digi-Sign and, in accordance with the law, to other persons;
- The Subscriber shall indemnify and at all time keep Digi-Sign fully indemnified for all loss and damage suffered by Digi-Sign resulting from:
  - all breach, non compliance or non observance of the terms and conditions in this CPS or in the Subscriber Application form; or
  - any fraud or deception committed by or other act of dishonesty of the Subscriber

### **3.1.3 Relying Party Obligations and Duties**

For the purpose of this CPS, the act of making use of an ID-Cert is referred to as reliance on the ID-Cert and the digital signature of the Subscriber. This relying party has a duty to decide whether to rely on the ID-Cert. Once this relying party has decided to do so, it has the obligation to:

- Understand the usage for which the ID-Cert is issued;
- Accept the responsibility to:
  - Check if an ID-Cert and its Issuer's Certificate have been suspended or revoked, and if an ID-Cert and its Issuer's Certificate have expired, before relying on it (The certificate status information can be retrieved from Digi-Sign Repository. Please refer to sections 3.1.4 and 3.7 for descriptions of the extent of Digi-Sign Repository.)
  - Verify the digital signature, including the performance of all appropriate ID-Cert path validation procedures
- Accept that the use of the ID-Cert is subject to applicable liability and warranty disclaimers outlined in section 3.2 herein;
- Accept that the use of Encipherment ID-Cert Class 3 is specifically for the limited purpose as outlined in Section 2.4 Community and Applicability.

### **3.1.4 Repository Obligations and Duties**

The Digi-Sign repository is a collection of databases available publicly for display and retrieval of the ID-Cert and related information. In providing the repository, Digi-Sign assumes the responsibility to:

- Publish the ID-Cert issued;
- Publish the Certificate Revocation List ("CRL"), and update this CRL promptly upon the suspension or revocation of an ID-Cert



- ❑ Provide a means of access to the Digi-Sign repository by the Subscribers, relying parties, and others who may be interested in the ID-Cert, or the public information regarding the Digi-Sign certification services;
- ❑ Publish the current and prior versions of this CPS; and
- ❑ Maintain the accessibility to the repository, except when it is necessary to suspend this access for maintenance or related reason.

Access to Digi-Sign Repository: <ldap.dg-sign.com>

### **3.2 Liabilities**

Unless otherwise stated in the terms and conditions specified in the Subscriber Application form and this CPS, Digi-Sign:

- ❑ Has no obligations to monitor the Subscribers in their use of the private key and ID-Cert;
- ❑ Undertakes no responsibility to notify relying parties of any changes in the circumstances relating to the Subscriber, or suspension and revocation of the ID-Cert after the Subscriber has used the private key or ID-Cert;
- ❑ Shall not be responsible for any liabilities arising from the use of a certificate that occurred in between the time when the Subscriber or the Authorized Delegate requests the revocation or suspension of the certificate and the time when Digi-Sign actually revokes or suspends the certificate;
- ❑ Shall not be responsible for any liabilities in the situation where a relying party is temporarily unable to obtain information on revoked certificates; and
- ❑ Is committed only to reasonable care and skill in performing its certification services.

Digi-Sign shall assume liabilities, responsibilities and duty of care to the extent as stipulated in this CPS and not any further. Digi-Sign has taken out insurance cover against claims arising from error or omission in relation to all Classes of ID-Cert. The amount of the insurance cover is in accordance with the relevant guidelines published by the Director of Information Technology Services.

In the event that any information contained in an ID-Cert is inaccurate or misleading, or any information herein or otherwise disclosed by Digi-Sign is misrepresented owing to the negligence or default of Digi-Sign, its employees or agents, Digi-Sign shall in any event not be liable to the Subscribers or any relying parties for loss or damage in excess of a Liability Cap of HK\$200,000.00 (“the Liability Cap”) in respect of one ID-Cert and irrespective of the number of transactions involved in that one ID-Cert.

Provided further that Digi-Sign may only incur liability up to the Liability Cap upon proof of loss, proof of negligence or default on the part of Digi-Sign and if the cause of such loss or damage is due to reasonable reliance on the inaccurate information, and is subject to the limitations on loss or damage prescribed in section 3.2.1 herein.

Digi-Sign employees, contractors, or other non Digi-Sign entities acting for or on behalf of Digi-Sign, are not parties to the terms and conditions specified in the Subscriber Application form, and none of them shall accept any responsibility in their own rights in any legal actions, claims, or forms of redress initiated by a Subscriber or relying party.



When an ID-Cert expires, or upon its revocation in accordance with this CPS, Digi-Sign's obligations and duties to the Subscriber under the terms and conditions specified in the Subscriber Application form and this CPS shall lapse without notice.

Save and except provided above, Digi-Sign shall assume no liability for any loss or damage howsoever suffered by the ID-Cert Subscriber or any relying parties in relation to the ID-Cert.

### **3.2.1 Disclaimers & Limitations on Warranties**

Except as expressly provided in the terms and conditions specified in the Subscriber Application Form and in this CPS, Digi-Sign disclaims warranties and obligations of any types, and in particular the fitness of use of an ID-Cert, private key, or software for a particular purpose.

### **3.2.2 Time Limitation**

Digi-Sign shall disclaim any liability to a Subscriber, or a relying party, who fails to make any legal claims arising from, or in connection with, the issuance, revocation or publication of an ID-Cert within twelve months of the date upon which the Subscriber or the relying party, as the case may be, becomes aware of the facts or circumstances giving rise to such claim. Where the Subscriber or relying party, upon reasonable care and diligence, should have been aware of such facts or circumstances at an earlier date, the above period of 12 months shall commence from such earlier date.

### **3.2.3 Other Exclusions**

Digi-Sign's warranty, liability, responsibility or obligations shall lapse upon any attempt by the Subscriber or relying party of the ID-Cert to circumvent duty, or any failure to observe obligations in the terms and conditions specified in the Subscriber Application form or in this CPS. Upon any of these occurrences, the right of the Subscribers and relying parties to make claims shall also lapse.

### **3.3 Reliance Limit**

Each ID-Cert shall contain and for all purposes be deemed to contain the following Notice and Reliance Limits:

*Pursuant to section 42(1) of the Electronic Transactions Ordinance (Cap.553), Digi-Sign is not liable for any loss caused by reliance on a false or forged digital signature of a Subscriber supported by an ID-Cert issued by Digi-Sign, if Digi-Sign has complied with the requirements of the Electronic Transactions Ordinance (Cap.553) and the relevant code of practice with respect to that ID-Cert.*

*The Reliance Limit for the purpose of section 42(2) of the Electronic Transactions Ordinance (Cap.553) is zero. Pursuant to section 42(2) of the Electronic Transactions Ordinance (Cap.553), Digi-Sign, is not liable in excess of the above Reliance Limit, for a loss caused by reliance on any information-*

*(a) that Digi-Sign is required to confirm according to the CPS and the relevant code of practice; and*



*(b) which is misrepresented on an ID-Cert or in a repository,*

*if Digi-Sign has, in relation to that ID-Cert, complied with the requirements of the Electronic Transactions Ordinance (Cap.553) and the relevant code of practice.*

### **3.4 Financial Responsibility**

Digi-Sign undertakes to maintain sufficient financial resources to carry on its certification services for a minimum period of 90 days. Furthermore, Digi-Sign has insured itself against claims due to errors and omissions.

### **3.5 Interpretation & Enforcement**

#### **3.5.1 Governing Law**

The laws of the HKSAR govern the enforceability, construction, interpretation, and validity of the terms and conditions specified in the Subscriber Application form and this CPS. Subscribers and relying parties shall agree to submit to the non-exclusive jurisdiction of the Courts of the HKSAR.

#### **3.5.2 Severability**

If any of the provisions in this CPS is declared or found to be invalid, illegal, unenforceable or void, then any offending words therein will be deleted to the extent necessary to make it valid, legal and enforceable while preserving the intent. In any event, the unenforceability of any of the provisions in this CPS will not impair the enforceability of any other provisions in this CPS.

#### **3.5.3 Survival**

Each and all of the provisions in this CPS shall be binding upon and shall inure to the benefit of the respective executors, administrators and personal representatives of the parties hereto.

#### **3.5.4 Notice**

Save and except otherwise provided herein, all notice, demand or other communication given or made pursuant to this CPS shall be given or made either using digitally signed electronic messages consistent with the requirements of this CPS or in writing. Communication by electronic communications shall be deemed to be effective upon the sender receiving a valid, digitally signed acknowledgment of receipt from the recipient. Such acknowledgment must be received within five (5) days, otherwise, the notice, demand or communication must be given or made in writing.

All written notice, demand or communication shall be delivered personally, or sent by mail, addressed to the party or parties to whom they are directed at their registered or last known address. Any notice, demand or other communication given or made by mail in the Hong Kong Special Administrative Region in the manner prescribed in this paragraph shall be deemed to have been received five (5) days after the date of mailing.



### **3.5.5 Agreement**

Save and except the terms and conditions specified in the Subscriber Application form entered between Digi-Sign and the Subscriber, the provisions in this CPS and all other documents expressly incorporated or referred herein constitute all understanding and agreement between Digi-Sign and the Subscriber. Any prior agreements, promises, negotiations, or representations not expressly set forth in this CPS and the terms and conditions specified in the Subscriber Application form shall be void and deemed to have been revoked.

### **3.5.6 Dispute Resolution**

A dispute or difference may arise from time to time between Digi-Sign and a Subscriber. Digi-Sign has established a series of steps to ensure that any complaints and claims arising from time to time are dealt with promptly. Subscribers or other users of Digi-Sign certification services are advised to call the Digi-Sign Hotline, if they wish to report any matters or make enquiries. Contact details are in section 1.2 herein.

Both Digi-Sign and its Subscribers undertake to make their best endeavours to resolve any dispute or difference within seven days from date of notice of a dispute or difference. Thereafter, any dispute or difference arising out of, or in connection with, the terms and conditions specified in the Subscriber Application form, or this CPS, shall be referred to the Hong Kong International Arbitration Centre (HKIAC) for mediation in accordance with its Mediation Rules.

If the mediation is abandoned by the mediator, or is otherwise concluded without resolution of the dispute or difference, then such dispute or difference may be referred to and determined by arbitration at HKIAC, and in accordance with its Domestic Arbitration Rules.

### **3.6 Fees**

Digi-Sign may determine its charges from time to time for processing the Subscriber Application, administration, and other types of services. A schedule of the current fees is available from the Digi-Sign Website at <[www.dg-sign.com](http://www.dg-sign.com)>. Digi-Sign reserves its right to change this schedule of fees from time to time. Digi-Sign further reserves its right to publish this schedule of fees by other means.

### **3.7 Publication & Repository**

Digi-Sign undertakes to publish in a public repository this CPS, list of ID-Cert issued, the CRL, the Digi-Sign public keys and ID-Certs, and other types of information as Digi-Sign may determine from time to time. Digi-Sign is responsible for updating the information in this repository as and when necessary. The content of this repository will be managed in accordance with the Digi-Sign information security policy, privacy and confidentiality guidelines and practices.

The Digi-Sign repository is available normally on a continuous basis 24 hours daily, excluding when it is shut down for scheduled routine maintenance of up to 2 hours weekly, during non-routine maintenance, or in an emergency. Digi-Sign reserves its absolute right to publish the information by other means.



Access to Digi-Sign Repository: ldap.dg-sign.com

### **3.8 Compliance Assessment**

The Digi-Sign certification services covered by this CPS are subject to periodic assessments by an independent assessor. Following the initial assessment performed in accordance with section 20 (3) (b) of the Electronic Transactions Ordinance (Cap. 553), assessments will be carried out once every 12 months from the date of the last assessment.

### **3.9 Confidentiality Policy**

Digi-Sign has established its confidentiality policy consistent with the Personal Data (Privacy) Ordinance (Cap. 486), and Electronic Transactions Ordinance (Cap. 553). Digi-Sign undertakes to display this policy on Website <[www.dg-sign.com](http://www.dg-sign.com)>. Digi-Sign reserves its right to publish this policy by other means.

### **3.10 Intellectual Property Rights**

Digi-Sign reserves all rights including, but not limited to, its intellectual property rights relating to the ID-Cert, CRL, terms and conditions specified in the Subscriber Application form, this CPS, specifications and names used in keys, and other types of information that Digi-Sign may publish from time to time.



## 4. IDENTIFICATION AND AUTHENTICATION

Digi-Sign is responsible for establishing the requirements for verification of the Subscriber Application. Digi-Sign reserves its absolute right to approve or reject a Subscriber Application without providing any explanations or reasons.

### 4.1 Initial Certification

Digi-Sign undertakes the necessary procedures to verify:

- The identity of each Personal ID-Cert Class 1 applicant; or
- The identity of each Organizational ID-Cert Class 2 applicant and validity of the authority to submit a Subscriber Application; or
- For each Encipherment ID-Cert Class 3 applicant-
  - The identity of the applicant if the applicant also applies for or holds a Personal ID-Cert Class 1;
  - The identity of the applicant and validity of the authority to submit a Subscriber Application if the applicant also applies for or holds an Organizational ID-Cert Class 2.

This verification is to be carried out according to the details received by Digi-Sign in the Subscriber Application. In doing so, Digi-Sign seeks to confirm, amongst others, the following:

- In the case of a Personal ID-Cert Class 1, that the personal identity published in the ID-Cert relates to the person named therein;
- In the case of an Organizational ID-Cert Class 2, that:
  - the organizational information relates to the organization named therein; and
  - the Subscriber Application is properly authorized.
- In the case of an Encipherment ID-Cert Class 3, that
  - For individuals, the personal identity published in the ID-Cert relates to the person named therein;
  - For organizations, the organizational information relates to the organization named therein, and the Subscriber Application is properly authorized.

Digi-Sign will carry out the verification against the Subscriber Application according to the class of ID-Cert, namely:

#### Personal ID-Cert Class 1

The Subscriber Application will be verified against the following on a face-to-face basis:

- (1) Where the applicant is a Hong Kong permanent resident, the Hong Kong permanent identity card; or
- (2) Where the applicant is not a Hong Kong permanent resident, the Hong Kong identity card, or a valid travel document, and this travel document must indicate that the holder's limit of stay in Hong Kong has not expired.



Digi-Sign requires the applicant in (1) and (2) above to produce information and document(s) to Digi-Sign to facilitate verification of the personal identity of the applicant in the processing of the Subscriber Application.

Where the personal particulars are made available to Digi-Sign through an Accredited Organization, the Subscriber Application will be verified against the personal details transferred from the Accredited Organization. Refer to section 2.2 for explanation of Accreditation of Organizations.

Digi-Sign reserves its absolute right to request the applicant to produce additional information and document(s) to facilitate verification of the personal identity of the applicant in the Subscriber Application, if Digi-Sign considers this necessary to substantiate further the information already available in specific cases.

### Organizational ID-Cert Class 2

The Subscriber Application will be verified against:

- ❑ The mandate / resolution substantiating the authority for the Subscriber Application;
- ❑ The search result of the business registration from the Inland Revenue Department, company registration from the Company Registry, or for organizations other than those registered with the Inland Revenue Department or the Company Registry, registration from the respective registration agency responsible for keeping the details; and
- ❑ In the case of a statutory body, the relevant legislation prescribing the establishment of the statutory body.

Applicants will be required to nominate an Authorized Delegate in the Subscriber Application. Where the Authorized Delegate is not yet a Personal ID-Cert Class 1 Subscriber, this Authorized Delegate will be required to produce information and document(s) to a Digi-Sign representative for the purpose of verification of the personal identity of the Authorized Delegate. Where the Authorized Delegate is already a Personal ID-Cert Class 1 Subscriber, verification of the personal identity of this person will not be required.

Digi-Sign will withhold issuance of an Organizational ID-Cert Class 2 until satisfactory verification is completed against the search results of the business registration, company registration, or other registration administered by a registration agency of the Government of Hong Kong SAR.

Where the Subscriber Application details are made available to Digi-Sign through an Accredited Organization, the Subscriber Application will be verified against the Subscriber Application details transferred from the Accredited Organization. Refer to section 2.2 for explanation of Accredited Organization. But Digi-Sign reserves its absolute right to carry out further verification in specific cases as follows:

- (1) the business registration should be subject to verification by search at the Inland Revenue Department; or
- (2) the company registration should be subject to verification by search at the Company Registry; or



- (3) other registration should be subject to verification by search of the records kept by the relevant registration agency.

### Encipherment ID-Cert Class 3

When the Subscriber Application is lodged at the same time as that for the Personal ID-Cert Class 1 or Organizational ID-Cert Class 2, as the case may be, the Subscriber Application will be verified in the process of verification of the Subscriber Application for Personal ID-Cert Class 1, or Organizational ID-Cert Class 2, respectively.

Where the Subscriber Application for Encipherment ID-Cert Class 3 is lodged separately, the applicant must be an existing holder of the Personal ID-Cert Class 1 or Organizational ID-Cert Class 2, the Subscriber Application will therefore be verified against the relevant personal or organizational identity particulars, as the case may be, kept by Digi-Sign.

In all cases, Digi-Sign reserves its absolute right to carry out all verification procedures and conduct all searches in any publicly available registries as Digi-Sign shall at its absolute discretion consider appropriate. Digi-Sign will request the Subscriber to reimburse all reasonable costs thereby incurred.

#### **4.1.1 Types of Names**

All names used must be in English. Digi-Sign does not currently support the use of names in other languages. To avoid duplication of names used, Digi-Sign will identify a Subscriber in an ID-Cert by a combination of the following elements recorded in the ID-Cert:

##### Personal ID-Cert Class 1

- (1) The particulars of the Issuer as specified in the ID-Cert Profile.
- (2) The Subscriber Name shown in the Personal ID-Cert Class 1 shall be identical to the name shown in one of the following documents used in support of the Subscriber Application:
  - Hong Kong permanent identity card;
  - Hong Kong identity card;
  - Valid travel document
- (3) The Class of ID-Cert
- (4) The Subscriber Number, as allocated by Digi-Sign after verification of the personal identity of the individual based on the name and identity card number, or travel document number.

##### Organizational ID-Cert Class 2

- (1) The particulars of the Issuer as specified in the ID-Cert Profile.
- (2) The Subscriber Name shown in the Organizational ID-Cert Class 2 shall be identical to the name used in the following:
  - Business registration;
  - Company registration; or
  - Other registration that is administered by a registration agency of the Government of Hong Kong SAR.



- (3) The Class of ID-Cert
- (4) The Subscriber Number, as allocated by Digi-Sign after verification of-
  - ❑ the identity of the organization based on search result of the business registration, company registration, or other registration from the respective registration agency responsible for keeping the details; or
  - ❑ the authorization letter in the case of bureau, department and agency of the Government of Hong Kong SAR.

### Encipherment ID-Cert Class 3

- (1) The particulars of the Issuer as specified in the ID-Cert Profile.
- (2) For individuals, the Subscriber Name shall be identical to the name shown in one of the following documents used in support of the Subscriber Application:
  - ❑ Hong Kong permanent identity card;
  - ❑ Hong Kong identity card;
  - ❑ Valid travel document

For organizations, the Subscriber Name shall be identical to the name shown in the Business Registration, Company Registration, or other registration that is administered by a registration agency of the Government of HKSAR.

- (3) The Class of ID-Cert
- (4) The Subscriber Number, as allocated by Digi-Sign after verification of:
  - ❑ In the case of an individual, the personal identity of the individual based on the name and identity card number, or travel document number;
  - ❑ In the case of an organization, the search result of the business registration, company registration, or other registration from the respective registration agency responsible for keeping the details; or
  - ❑ In the case of bureau, department and agency of the Government of HKSAR, the authorization letter.
- (5) Email address provided by the Subscriber.

#### **4.1.2 Need for Meaningful Name**

For the purpose of determining the identity of a Subscriber, the four elements as indicated in 4.1.1 must be used together as they are shown in the relevant ID-Cert.



### 4.1.3 Rules for Interpreting Various Name Formats

Interpretation of the name formats in an ID-Cert issued under this CPS will be as follows:

<b>Type</b>	Recognized Certificate	Recognized Certificate	Recognized Certificate
<b>Class</b>	Personal ID-Cert Class 1	Organizational ID-Cert Class 2	Encipherment ID-Cert Class 3
<b>Description</b>	Subscriber must be an individual – refer to section 4.1 herein	Subscriber must be a company, organization, or a statutory body – refer to section 4.1 herein	Subscriber must be an individual, company, organization, etc. – refer to section 4.1 herein
<b>Issuer</b>	c = HK o = Digi-Sign Certification Services Limited ou = (BR No. of Digi-Sign) cn = (Digi-Sign sub CA)	c = HK o = Digi-Sign Certification Services Limited ou = (BR No. of Digi-Sign) cn = (Digi-Sign sub CA)	c = HK o = Digi-Sign Certification Services Limited ou = (BR No. of Digi-Sign) cn = (Digi-Sign sub CA)



<b>Subject Name</b>	c = HK o = class of ID-Cert (certificate request number assigned by CA) ou = Subscriber number cn = name of Subscriber as shown in respective identity document	c = HK o = class of ID-Cert (certificate request number assigned by CA) ou = name of registered organization and Business Registration Number, or, Number of Certificate of Incorporation, or Number of Certificate of Registration, or Two-character Country Code <sup>4</sup> (where the organization is incorporated in) and other identification and Subscriber number cn = name of authorized delegate	c = HK o = class of ID-Cert (certificate request number assigned by CA) ou = name of individual as shown in respective identity document in the case of an individual being the applicant, or name of registered organization in the case of an organization being the applicant and Subscriber number cn = email address as provided by Subscriber
---------------------	--	--	--

#### 4.1.4 Uniqueness of Names

The four elements relating to the Personal ID-Cert Class 1 as described in 4.1.1 must be used together to produce a unique name of the individual covered by a Personal ID-Cert Class 1. Similarly, the four elements relating to the Organizational ID-Cert Class 2 as described in 4.1.1 must be used together to produce a unique name of the organization covered by an Organizational ID-Cert Class 2.

#### 4.1.5 Name Dispute Resolution Procedures

Digi-Sign has the sole absolute right on and shall be solely responsible for determining any name dispute. The decision of Digi-Sign shall be final.

#### 4.1.6 Verification of Subscriber Identity

Description of the verification procedures is outlined in section 4.1 herein. The Subscriber details completed in the Subscriber Application will be verified. This verification will include:

<sup>4</sup> The Two-character Country Code follows the international standard ISO 3166-1. Information about ISO 3166-1 can be found at <[www.iso.org](http://www.iso.org)>. The ISO 3166 Country Code list can be found at <[www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html](http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html)>



- ❑ In the case of a Personal ID-Cert Class 1, verification of the Subscriber's personal identity;
- ❑ In the case of an Organizational ID-Cert Class 2, verification of the Subscriber's identity as an entity, and the authority for the Subscriber Application;
- ❑ In the case of an Encipherment ID-Cert Class 3, where the Subscriber is an individual, verification of his / her personal identity, and where the Subscriber is an organization, verification of the Subscriber's identity as an entity, and the authority for the Subscriber Application.

#### **4.1.7 Method of Proof of Possession of Private Key**

Digi-Sign is solely responsible for key generation, and this is done centrally within the Digi-Sign premises, and in the Digi-Sign trustworthy system. Upon generation, the private key and ID-Cert will be stored on appropriate storage media for dispatch to the Subscriber, and this will be done in a secure manner. There will be segregation of duties to generate the private key, copy the keys to the storage medium, generate the PIN, and print the PIN Mailer. The storage medium containing the private key and the ID-Cert, and the PIN Mailer will be dispatched to the Subscriber as described in section 5.2.2.

#### **4.1.8 Online Applications**

ID-Cert Class 1 and the corresponding ID-Cert Class 3 can also be applied online at Digi-Sign Web site <[www.dg-sign.com](http://www.dg-sign.com)>. If an ID-Cert Class 1 application (may optionally include the ID-Cert Class 3 application) is submitted online, Digi-Sign will, upon receiving the Subscriber Application, contact the applicant to confirm the personal identity details on the Subscriber Application, and the following documents will be verified against the Subscriber Application subsequently through a face-to-face interview with the applicant:

- (1) In case the applicant is a Hong Kong permanent resident, the Hong Kong permanent identity card; or
- (2) In case the applicant is not a Hong Kong permanent resident, the Hong Kong identity card, or a valid travel document, and this travel document must indicate that the holder's limit of stay in Hong Kong has not expired.

Digi-Sign requires the applicant in (1) and (2) above to produce information and document(s) stated above to Digi-Sign to facilitate verification of the personal identity of the applicant in the processing of the Subscriber Application.

Digi-Sign reserves its absolute right to request the applicant to produce additional information and document(s) to facilitate verification of the personal identity of the applicant in the Subscriber Application, if Digi-Sign considers this necessary to substantiate further the information already available in specific cases.

## **4.2 Certificate Renewal**

Digi-Sign does not renew an ID-Cert. Upon approval of the application submitted by the Subscriber, Digi-Sign will generate new Subscriber private key and ID-Cert as replacement before expiry of the Subscriber's existing private key and ID-Cert.



Before an ID-Cert is due to expire, Digi-Sign will issue an expiry notice to the Subscriber. It will be up to the Subscriber to apply, and this should be done before the existing ID-Cert expiry date.

Digi-Sign will be responsible to verify the application against the information held in the Digi-Sign Subscriber database. But Digi-Sign reserves its absolute right to request the Subscriber to provide further proof as follows:

- In the case of a Personal ID-Cert Class 1, proof of personal identity;
- In the case of an Organizational ID-Cert Class 2, proof of registration to substantiate the identity of the organization, and the authority for the application;
- In the case of an Encipherment ID-Cert Class 3-
  - Proof of personal identity if the Subscriber also holds a Personal ID-Cert Class 1;
  - Proof of registration to substantiate the identity of the organization, and the authority for the application if the Subscriber also holds an Organizational ID-Cert Class 2.

Digi-Sign reserves its absolute right to refuse the Subscriber's application if the Subscriber fails to provide the proof as requested by Digi-Sign.

Upon approval of the application, Digi-Sign will generate a new key pair and ID-Cert for the Subscriber. Digi-Sign will follow the procedures in sections 5.2.2 and 5.2.3 as a means of confirmation of the receipt of the new key pair and ID-Cert by the Subscriber.

Nothing in this CPS shall constitute any agreement or promise on the part of Digi-Sign or an option available to the Subscriber to apply for a new ID-Cert to replace the one due to expire soon. Digi-Sign reserves its absolute right to refuse the Subscriber's application or issuance of ID-Cert without giving any reasons.

### **4.3 Application After Revocation**

If the Subscriber requires the use of an ID-Cert after revocation, it will be necessary for the Subscriber to submit a new Subscriber Application. Digi-Sign will deal with this Subscriber Application in accordance with section 4.1 herein. As explained in section 4.2, Digi-Sign does not re-use a Subscriber's private key.



#### 4.4 Revocation Request

Digi-Sign will revoke an ID-Cert if:

- ❑ Digi-Sign has determined that it is necessary to do so; or
- ❑ The Subscriber has requested Digi-Sign to do so.

(a) Revocation as determined by Digi-Sign

Digi-Sign may decide to revoke an ID-Cert in certain circumstances including, but not limited to, when:

- (1) It is required to revoke the ID-Cert by regulations, or by law:
- (2) It is determined that the ID-Cert:
  - ❑ was issued improperly, or was not issued in accordance with this CPS
  - ❑ includes incorrect or untrue information;
- (3) It is determined that the Subscriber:
  - ❑ has passed away
  - ❑ has become an undischarged bankrupt, or has entered into a composition or scheme of arrangement, or a voluntary arrangement within the meaning of the Bankruptcy Ordinance (Cap. 6)
  - ❑ has been convicted in Hong Kong or elsewhere of an offence for which the Subscriber has been found to have acted fraudulently, corruptly, or dishonestly, or committed an offence under the Electronic Transactions Ordinance (Cap. 553)
- (4) It is established, or it is reasonable to suspect, that:
  - ❑ the private key of a Subscriber has been compromised;
  - ❑ the Subscriber is not using the private key or ID-Cert in accordance with this CPS;
  - ❑ the Subscriber has failed to meet the Subscriber obligations set out in this CPS;
- (5) In the case of an Organizational ID-Cert Class 2 and Encipherment ID-Cert Class 3 in the name of the holder of an Organizational ID-Cert Class 2, it is established that:
  - ❑ the Subscriber is in liquidation, or a winding up order relating to the Subscriber has been made by any Court of competent jurisdiction;
  - ❑ a receiver or administrator has been appointed over any part of the Subscriber's assets;
  - ❑ a director, or public officer of the Subscriber has been convicted of an offence under the Electronic Transactions Ordinance (Cap. 553).

The decision of Digi-Sign on revocation of an ID-Cert will be final and there will not be any appeal. Subscribers and relying parties should take note of the period between the processing of a revocation request and updating of the Digi-Sign CRL as set out in the following paragraphs. Digi-Sign shall not be liable for loss or damage suffered by the Subscriber or any third party as a result of the revocation of an ID-Cert by Digi-Sign.



(b) Revocation at request of the Subscriber

The Subscribers may at any time apply to Digi-Sign to revoke the ID-Cert. However, a Subscriber must promptly apply to Digi-Sign to revoke the ID-Cert upon the occurrence of the following:

- ❑ Loss of the private key
- ❑ Compromise or suspected compromise of the private key
- ❑ Failure of the protection of the private key, or suspected failure of the protection

A request to revoke an ID-Cert must be in writing and submitted by the Subscriber to Digi-Sign either electronically, or in person. Digi-Sign will provide facilities for the Subscriber to:

- ❑ Download a revocation request form: or
- ❑ Key in the revocation request for sending to Digi-Sign online.

Digi-Sign will keep records of the time and date of receipt of a revocation request, and endeavour to process the revocation before the end of the next working day of its receipt at the Digi-Sign Office. Processing of the request will include checking of:

- ❑ The Subscriber's signature in the revocation request form, or
- ❑ The Subscriber's digital signature, where the revocation request is sent electronically.

Once the validity of the revocation request is established, Digi-Sign will initiate action in its trustworthy system to revoke the ID-Cert, and update the CRL. The business hours for processing of ID-Cert Revocation Request are as follows:

Monday to Friday:	8:30am to 5:30pm
Saturday:	8:30am to 12:30pm

Whenever it is necessary to notify Digi-Sign of an ID-Cert Revocation Request outside the above business hours, or on any day when the Digi-Sign Office is closed for business, the Subscriber should call the Emergency Telephone No. in section 1.2 herein to make arrangement.

(c) For all revocation of ID-Cert

The Digi-Sign trustworthy system will update the Digi-Sign CRL promptly upon the processing of revocation of an ID-Cert in the system. Digi-Sign will further issue a notice of revocation to the Subscriber, and this will be done within two working days of the update of the revocation to the CRL.

#### 4.5 Suspension Request

Digi-Sign does not process requests by Subscribers to suspend the use of an ID-Cert. However, Digi-Sign may initiate an entry in the Digi-Sign trustworthy system to suspend an ID-Cert. This may occur when it is necessary to suspend an ID-Cert, pending validation of:

- ❑ A revocation request received by Digi-Sign; or
- ❑ Any information received by Digi-Sign suggesting that revocation of an ID-Cert may be necessary.



When an ID-Cert is suspended, the CRL will be updated with the appropriate reason code. The suspension period of an ID-Cert is 3 months, pending validation as described above. Depending on the result of the validation, Digi-Sign may either cancel the suspension and re-activate the ID-Cert, or if necessary, suspend the ID-Cert, or revoke the ID-Cert. Following the expiry of the suspension period, Digi-Sign may either re-activate the ID-Cert, or if necessary, suspend the ID-Cert, or revoke the ID-Cert. The decision of Digi-Sign to suspend an ID-Cert will be final and there will not be any appeal. Digi-Sign shall not be liable for loss or damage suffered by the Subscriber or any third party as a result of the suspension of an ID-Cert by Digi-Sign.



## 5. OPERATIONAL REQUIREMENTS

Digi-Sign establishes as part of its trustworthy system procedures to process Subscriber Applications, ID-Cert issuance, acceptance, and revocation.

### 5.1 Subscriber Application

Upon submitting a Subscriber Application, the applicant warrants to Digi-Sign that the information provided is true and correct, and when requested to do so, provides further proof to substantiate the details completed therein.

It is the responsibility of the applicant to lodge the Subscriber Application at the Digi-Sign Office, or with a Digi-Sign representative. Digi-Sign will undertake to notify the applicant of the result of the Subscriber Application within three working days of the decision to approve or reject the Subscriber Application.

Digi-Sign reserves its absolute right to change the procedures to process the Subscriber Application from time to time without notice.

Subscriber Application for ID-Cert must be completed in a form provided by Digi-Sign. This form is available from the Digi-Sign Office, or may be downloaded from the Digi-Sign Website.

### 5.2 Certificate Issuance

Digi-Sign is solely responsible for processing the Subscriber Applications for the purpose of generating the keys and ID-Cert centrally within the Digi-Sign premises and in the Digi-Sign trustworthy system.

#### 5.2.1 Key Generation

Digi-Sign will process the key and ID-Cert generation upon completion of the verification of the Subscriber Application. The keys and ID-Cert generated will be in PKCS#12 format and stored on a floppy disk for delivery to the Subscriber. Digi-Sign is committed to expanding the variety of suitable storage media for this purpose.

#### 5.2.2 Delivery of Keys

Digi-Sign will create a secure packet to keep the floppy disk, issue a Letter of Acceptance to request the Subscriber to confirm the information published in the ID-Cert; issue an acknowledgement letter to request the Subscriber to confirm the receipt of the secure packet and print out a PIN Mailer for the Subscriber. This secure packet will be available for collection by the Subscriber in person. The Subscriber may request Digi-Sign to courier this secure packet to the Subscriber.

Upon the collection of the secure packet, the Subscriber will need to sign off the Letter of Acceptance to confirm the information published in the ID-Cert. The Subscriber will then check the secure packet to see whether it is intact or tampered with. The Subscriber will then sign off the acknowledgement letter to confirm the receipt of the secure packet. PIN Mailer



will then be handed over to the Subscriber. Upon issuance of the Subscriber's private key and PIN, Digi-Sign does not retain copies of the Subscriber's private key and PIN.

In the event of any doubt as to the completion of the above procedures, or any suspicion that the secure packet has been tampered with, Digi-Sign will undertake to revoke the keys and ID-Cert and then proceed to generate a new set of keys and ID-Cert for the Subscriber.

### **5.3 Certificate Acceptance**

#### **5.3.1 Responsibility of Subscriber**

By signing the Letter of Acceptance, the Subscriber has:

- accepted the private key and ID-Cert;
- confirmed that the personal information contained in the ID-Cert is correct; and
- accepted that Digi-Sign has the authority to display the ID-Cert in the repository .

#### **5.3.2 Notification of Change**

If the Subscriber information published in the ID-Cert is no longer correct, or the information supplied by the Subscriber has changed since the Subscriber Application was made to Digi-Sign, the Subscriber undertakes to inform Digi-Sign immediately. Digi-Sign shall decide upon what further action is necessary.

### **5.4 Certificate Suspension & Revocation**

#### **5.4.1 Certificate Suspension**

Digi-Sign may exercise its discretion to suspend an ID-Cert. Please refer to section 4.5 for explanation of the use of this option.

#### **5.4.2 Updating of the CRL**

For every ID-Cert revoked or suspended in the procedures in section 4.4 and section 4.5 respectively, the ID-Cert information, together with the reason code indicating the reason for which the ID-Cert has been revoked or suspended, as the case may be, will be updated to the Digi-Sign CRL. Digi-Sign undertakes to update the CRL daily. Please refer to section 3.2 for description of the extent of Digi-Sign's liabilities.

### **5.5 Security Review Procedures**

The Digi-Sign Information Security Guidelines and Practices provides guidance relating to the following:

- Monitoring of system access and use
- Security monitoring
- Security audit and review

Specific information relevant to Digi-Sign certification services operation is outlined below:



### **5.5.1 Event Logging**

Digi-Sign will maintain record of events relating to its day-to-day operations including, but not limited to, the following:

- ❑ Suspicious network activity;
- ❑ Repeatedly failed attempts to access;
- ❑ Events related to the operation of the Digi-Sign trustworthy system;
- ❑ Access control
- ❑ ID-Cert certificate management operations, such as:
  - ID-Cert issuance and acceptance
  - ID-Cert revocation
  - ID-Cert suspension
  - CRL update and display
  - Repository update
  - Digi-Sign CA key rollover
  - Backup and restore from backup

### **5.5.2 Frequency of Processing Log**

Digi-Sign will update its processing log daily to keep track of the processes in the Digi-Sign trustworthy system.

### **5.5.3 Retention Period for Processing Log**

In accordance with the Digi-Sign Information and Records Retention Policy, processing logs will be kept for seven years from date of entry in the log.

### **5.5.4 Protection of Processing Log**

The Digi-Sign trustworthy system incorporates appropriate internal control described in the Digi-Sign Information Security Guidelines and Practices. These guidelines and practices will provide the necessary steps to maintain protection of the records in the processing log.

### **5.5.5 Backup of Processing Log**

The Digi-Sign trustworthy system incorporates appropriate internal control described in the Digi-Sign Information Security Guidelines and Practices. These guidelines and practices will provide the necessary steps to maintain formal backup of the processing log, including storage of the backup copies, and procedures to restore from backup, whenever this becomes necessary.



## **5.6 Information and Record Archival**

The general rule is that there will be:

- ❑ Sufficient details kept in the Digi-Sign archive to establish the validity and authenticity of the ID-Cert; and
- ❑ Sufficient evidence to substantiate the proper operation of Digi-Sign trustworthy system, past and present.

The Digi-Sign trustworthy system provides for the following to be retained in its archival records:

- ❑ System and equipment configuration;
- ❑ Results of assessments and / or reviews for accreditation of the equipment;
- ❑ Certification practice statement;
- ❑ Contractual agreements entered by Digi-Sign;
- ❑ Modifications or updates to any of the above;
- ❑ All public key certificates issued and all CRLs published;
- ❑ Digi-Sign trustworthy system processing log;
- ❑ Other data necessary for verification of the archive;
- ❑ Versions of software such that the archival records and information can be accessed and used.

### **5.6.1 Retention Period**

The Digi-Sign Information and Records Retention Policy provides the direction for keeping of Subscriber and ID-Cert details and archival records for seven years following the ID-Cert expiry date or revocation date. There will be audit trails, which may be deemed to be sufficient to keep track of those archival records.

### **5.6.2 Protection of Archive**

Digi-Sign undertakes to keep archival records under protection to the extent that it is commercially viable against undesirable events, such as accidental destruction or deliberate modification, theft, or media degradation. In addition, Digi-Sign has procedures in place to:

- ❑ Restrict access for approved review and retrieval of information or records; and
- ❑ Protect the information and records from loss or destruction.

### **5.6.3 Archive Backup Procedures**

For data generated in the course of the Digi-Sign certification services operation, there will be backup copies kept at the respective off-site storage locations. The Digi-Sign Information Security Guidelines and Practices will be followed in handling of backup data.

## **5.7 Key Changeover**



The Digi-Sign keys and certificates have a predetermined life span. Digi-Sign has set its key and certificate life cycle management plan as outlined in Appendix 3.

The Digi-Sign keys and certificates will be scheduled for replacement promptly prior to their respective expiry dates. Digi-Sign will:

- ❑ Display the details of these certificates in the repository; and
- ❑ Keep the original CA keys in safe custody for a minimum of seven years subsequent to their respective expiry dates.

## **5.8 CA Key Management**

Digi-Sign has established an appropriate management framework and procedures to securely manage its CA keys, including the keys for the Root CA and the signing CA. A specific document sets out the Digi-Sign CA Key Management Procedures, covering the processes, controls and responsibilities.

## **5.9 Key Compromise and Disaster Recovery**

The Digi-Sign Information Security Guidelines and Practices sets the direction for business continuity management, which encompasses the planning for recovery of the relevant systems and data, inclusive of the key, certificate information and records. The Digi-Sign business continuity plan also provides timely notification to the Director of Information Technology Services and the Subscribers of each occurrence of:

- ❑ Actual or suspected key compromise, and
- ❑ Issuance of replacement keys and certificates.

Digi-Sign further undertakes to notify the Director of Information Technology Services promptly upon activation of the business continuity plan. In doing so, Digi-Sign will make appropriate public announcement as to how it proposes to maintain the certification services.

## **5.10 Termination of CA Operations**

For the purpose of smooth and orderly transition, Digi-Sign has established appropriate procedures to deal with any need to withdraw its certification services and transfer its responsibilities as a Recognized Certification Authority to another entity in accordance with the Digi-Sign Termination Plan. These procedures will include revocation of all keys prior to termination of the CA operations.



## **6. PHYSICAL, PROCEDURAL & PERSONNEL SECURITY CONTROLS**

Digi-Sign has in place a risk management program consistent with the framework set out in the Risk Management Standard (AS 4360:1999) and Information Security Management Standard (BS 7799:1999) to manage risk and security.

The risk and security management framework established by Digi-Sign sets the necessary controls focusing, amongst others:

- Physical security controls
- Procedural controls
- Personnel security controls

### **6.1 Physical Security**

The Digi-Sign Information Security Guidelines and Practices sets the direction for protecting the physical security of its resources including, amongst others, its offices, data centres, computers and related equipment to the extent that is commercially viable and appropriate for carrying on the business of a Recognized Certification Authority. Specific focal areas include the following:

#### **(a) Site Location and Construction**

The focus is to address the needs relating to physical and environmental security, access control, business continuity management, and information and records retention.

The Digi-Sign Offices are at locations that are specially fitted out for the certification services operation. The physical lay out is documented and recorded with description of the control measures in place. Digi-Sign has further established the responsibility to administer security and monitor controls in the target areas outlined in the ensuing sections.

#### **(b) Access Controls**

Digi-Sign has set up commercially cost effective and reasonable access controls as a means of restricting access to the Digi-Sign trustworthy system. This restriction is based on the needs of the individuals within Digi-Sign to access the specific items of equipment to carry out their roles in the certification services operation. Access is controlled electronically and manually, and is monitored for unauthorized entry and intrusion at all times.

#### **(c) Power and Air Conditioning**

The Digi-Sign Offices and computer installations are serviced by standard power supply and air conditioning. These are supplemented by back up facility inclusive of uninterruptable power supply, and dedicated air conditioning.



(d) Water Exposure

Fitting out is done in a manner that takes into account appropriate and commercially viable measures to prevent damage due to water, and other threats due to nature. Digi-Sign has further put in place a plan to manage risk associated with natural events, including risk mitigation measures that are reasonably possible and commercially viable against damage due to natural events.

(e) Fire Prevention and Protection

Digi-Sign adopts commercial fire prevention and protection measures including, installation of fire fighting equipment and smoke detectors.

(f) Media Storage

Digi-Sign adopts commercially viable security practices, including the use of fireproof data safes.

(g) Waste Disposal

Digi-Sign has established secure disposal arrangement for removal and disposal of sensitive paper documents and magnetic media.

(h) Off-site Backup

Digi-Sign has established off-site storage facility for safe custody of backup software and data.

## 6.2 Procedural Controls

The Digi-Sign trustworthy system includes procedures and responsibility for carrying out these procedures with appropriate procedural controls to, wherever possible, safeguard against intentional manipulation or unintentional errors. The objective is to maintain accuracy and integrity of the certification services operation. The Digi-Sign trustworthy system addresses a number of focal areas, including the following:

(a) Trusted Roles

Digi-Sign personnel are given trusted roles in the Digi-Sign trustworthy system. The Digi-Sign trustworthy system is documented and is available for reference by Digi-Sign personnel on a “need to know” basis.

(b) Division of Duties

The Digi-Sign trustworthy system is set up in such a manner that an individual will not be placed in a position to violate internal control and integrity of the transaction.

## 6.3 Personnel Security Controls

The Digi-Sign Information Security Guidelines and Practices sets the direction for personnel security, which addresses security at the recruitment stage through to employment conditions,



service contracts and supervisory monitoring of employees, contractors and consultants. Digi-Sign further addresses personnel security by defining the scope and duty of each position, and how it fits into the overall organization structure. All Digi-Sign personnel, including employees, contractors and consultants are required to acknowledge their duty of compliance with the Digi-Sign Code of Ethics and Conduct.

Specific steps to maintain personnel security controls include the following:

(a) Background and qualifications

Digi-Sign has established appropriate recruitment and selection procedures, which require evaluation of, amongst other things, the candidate's personal background, academic and technical qualifications, experience, reference and "fit and proper person" clearance. The results have to be matched against the established requirements for a particular position.

(b) Background checks

Digi-Sign has established a requirement for all personnel in trusted roles to be a "fit and proper" person. Digi-Sign assesses each of the relevant personnel before engagement, and thereafter, periodically in the term of employment. In this context, Digi-Sign may require an individual to provide a self-declaration to the effect that he/she is a fit and proper person for the purpose of section 21(5) of the Electronic Transactions Ordinance (Cap. 553). Supervisory personnel of the Accredited Organization directly involved in the hand-over of PIN Mailers will be required by Digi-Sign to provide a self declaration to the effect that he / she is a fit and proper person for the purpose of section 21(5) of the Electronic Transactions Ordinance (Cap. 553).

(c) Training

The Digi-Sign Information Security Guidelines and Practices sets the direction for education and training of personnel. An ongoing program is in place to address security awareness and training needs.

(d) Performance assessment, disciplinary and termination procedures

Digi-Sign has an ongoing staff appraisal program as a means of evaluation of the performance of an individual in carrying out the duties and responsibilities. The Digi-Sign Information Security Guidelines and Practices further sets the direction for disciplinary action and termination procedures respectively.

(e) Documentation supplied to personnel

Individual Digi-Sign personnel are given access to the relevant Digi-Sign policies, guidelines and practices as well as documentation of the Digi-Sign trustworthy system. This access will be arranged for individuals on a "need to know" basis.



## 7. TECHNICAL SECURITY CONTROLS

Digi-Sign defines the technical security measures established to specifically protect its cryptographic keys and activation data.

The Digi-Sign Root CA keys are stored in hardware devices and are subject to access control. Use of these keys requires the approval of two authorizers.

### 7.1 Key Pair Generation and Installation

The Digi-Sign CA Key Management Procedures sets out the processes, controls and responsibilities for the generation and installation of the Digi-Sign CA key pairs. Elements of the Digi-Sign CA Key Management framework and the Subscriber key management are outlined below:

(a) Digi-Sign Root CA key pair and CA key pair generation and installation

The Digi-Sign Root CA keys and CA keys are generated and installed by Digi-Sign in accordance with the established procedures, requiring the presence of two authorizers to supervise the generation, installation, and access processes.

(b) Subscriber key pair generation

Subscriber key pairs are generated in accordance with the procedures in this CPS. This is done centrally within the Digi-Sign premises and in the Digi-Sign trustworthy system. There will be segregation of duties to generate the keys, copy the key and ID-Cert to the storage medium, generate the PIN and print the PIN Mailer.

(c) Subscriber key pair delivery

Refer to section 5.2.2 regarding the procedures to deliver the Subscriber private key and ID-Cert.

(d) Digi-Sign CA public keys

The public keys of all Digi-Sign CA key pairs are published in the Digi-Sign Website <[www.dg-sign.com](http://www.dg-sign.com)>.

(e) Key size

Each of the Digi-Sign CA key pairs is 2048-bit RSA. Subscriber key pairs are 1024-bit RSA in size.

(f) Key usage

The Digi-Sign CA keys are used for signing:

- ID-Cert; and
- CRL



Refer to section 2.5 herein for usage of Personal ID-Cert Class 1, Organizational ID-Cert Class 2, and Encipherment ID-Cert Class 3.

(g) Public key parameters generation

The parameters used to create public keys are generated by the Digi-Sign application.

(h) Parameter Quality Checking

The Digi-Sign application that generates the keys automatically checks the quality of the public key parameters.

(i) Cryptographic modules

The cryptographic module used in the Digi-Sign certification services operation is installed in the hardware and software within the Digi-Sign trustworthy system.

## 7.2 Digi-Sign CA Private Keys Protection

The Digi-Sign CA Key Management Procedures also sets out the processes, controls and responsibilities for the protection of the Digi-Sign CA private keys. The Digi-Sign Information Security Guidelines and Practices further sets the direction for accountability for information assets. Elements of the protection of the security of the Digi-Sign CA private keys are outlined below:

(a) Standards of cryptographic modules

The Digi-Sign Root CA private key is created in cryptographic modules designed to FIPS 140-1 Level 4 tamper resistance.

(b) Private key multi-person control

The use of Digi-Sign CA keys is subject to the established access control. Use of Digi-Sign CA keys on each occasion, backup or archival of the Digi-Sign CA keys are subject to the approval of two authorizers.

(c) Private key escrow

There is no plan at this time for Digi-Sign to support key escrow.

(d) Digi-Sign CA private keys backup

Digi-Sign undertakes to store the Digi-Sign CA private key in an encrypted form, and keep backup copies on-site and off-site in secure data storage facility.

(e) Digi-Sign CA private keys archival

The Digi-Sign Root CA key pair and other CA key pairs each has a life span determined in the Digi-Sign key and certificate life cycle management plan as outlined in Appendix 3. Upon



expiry, or revocation of any of the Digi-Sign CA keys and certificates, Digi-Sign will undertake to archive the Digi-Sign CA private key in a suitable storage device and keep in safe custody in archive for seven years.

(f) Digi-Sign CA private key entry in cryptographic module

The Digi-Sign Root CA private key is generated and stored in the hardware cryptographic module. The private key is in an encrypted form. It should be decrypted only when it is properly activated, and within the hardware cryptographic module.

(g) Method of activation and deactivation of Digi-Sign CA private key

The Digi-Sign CA private key is activated for use by properly completing the activation process, which requires two authorized users to enter their passphrase individually to access the activation data.

Upon termination of the Digi-Sign application using the private key, the system will automatically deactivate the private key.

(h) Revocation of Digi-Sign CA private key

Control of the CA keys is set out in the document “CA Key Management” covering, amongst others, initialization of the CA key tokens and revocation of the CA public keys.

### 7.3 Activation Data

Upon generation of the Digi-Sign private key, the system also generates activation data to protect the private keys. Access to such activation data requires the login by two authorized users.

### 7.4 Computer Security Controls

The Digi-Sign Information Security Guidelines and Practices sets the direction for protection of the security of the Digi-Sign private key activation data. The protection aims at prevention and detection of unauthorized access, modification, or compromise of the Digi-Sign trustworthy system.

### 7.5 Public Key Archival

Archival of all public keys issued by Digi-Sign is performed as specified in section 5.6.

### 7.6 System Development Life Cycle Controls

The Digi-Sign Information Security Guidelines and Practices sets the direction for:

- ❑ Acquisition, development and implementation of hardware and software for the Digi-Sign trustworthy system; and
- ❑ Maintenance of the Digi-Sign trustworthy system.



## **7.7 Network Security Controls**

The Digi-Sign Information Security Guidelines and Practices sets the direction for network management and control including, amongst others, network management, access, and Internet access and usage.

## **7.8 Cryptographic Module Engineering Controls**

The Digi-Sign trustworthy system includes use of cryptographic devices which are designed to FIPS 140-1 Level 4 tamper resistance.



## 8. CERTIFICATE AND CRL PROFILES

Digi-Sign establishes specifications of the ID-Cert format, and the CRL format, which indicates, amongst others, the ID-Cert profile information, and the CRL profile information.

### 8.1 Certificate Profile

The ID-Cert that bears the reference of this CPS contains the public key used for:

- Verification of the digital signature related to a document, electronic mail, or electronic transaction (in case of Class 1 and Class 2 ID-Cert);
- Verification of the digital signature related to lodgment of compliance information (in case of Class 1 and Class 2 ID-Cert);
- Encryption of a document, electronic mail or electronic transaction (in case of Class 3 ID-Cert);
- Verification of the digital signature related to an acknowledgement of receipt of encrypted message (in case of Class 3 ID-Cert);
- Proof of identity or other significant characteristics<sup>5</sup> of the Subscriber

Profiles of the various classes of ID-Cert are included in Appendix 1.

### 8.2 CRL Profile

Profile of the Digi-Sign CRL is included in Appendix 2.

---

<sup>5</sup> For details regarding the other significant characteristics, please refer to Subject Alternative Name of the Certification Specification of the corresponding class of ID-Cert in Appendix 1



## 9. CPS ADMINISTRATION

The Digi-Sign Management Committee is responsible for the preparation, revision and publication of this CPS. This CPS is subject to document control, which requires the official copy to be printed in original only.

The Digi-Sign Management Committee is responsible for establishing this CPS, setting the direction for the overall public key infrastructure and the certification services. Refer to section 1.2 for contact details.

This version of the CPS bears OID: 1.3.6.1.4.1.8420.1.1.11. This CPS is available from the Digi-Sign Office, the Digi-Sign Website at <[www.dg-sign.com](http://www.dg-sign.com)>, and the Digi-Sign public repository. It is a requirement that this CPS is binding on all ID-Cert Subscribers.

The Digi-Sign Management Committee is responsible for reviewing and approving any changes or variations to be made to this CPS. Digi-Sign is required to notify the Director of Information Technology Services of any changes or variations, and this must be done at least 7 days prior to the publication of the changes made.

Copies of this version and an earlier version of this CPS are available for review in the Digi-Sign Website referenced above.





## 10. INTEROPERABILITY

Digi-Sign adopts technical standards and management practices that are commonly in use and this facilitates interoperability whenever this becomes necessary.

Digi-Sign supports and promotes interoperability. Digi-Sign undertakes to follow Public Key Infrastructure industry standards including, but not limited to, the X.509v3 certificates, X.509v2 CRL, X.500 directory, LDAPv3 protocol, PKCS#11 and PKCS#12 key formats.



## 11. GLOSSARY OF TERMS

The terms in this CPS are defined as follows:

**“Accept an ID-Cert”** in relation to a person to whom an ID-Cert is issued, means that the person while having notice of the contents of the ID-Cert:

- a) authorizes the publication of the ID-Cert to one or more persons or in a repository;
- b) uses the ID-Cert; or
- c) otherwise demonstrates approval of the ID-Cert.

**“Accredited Organization”** refers to an organization which has been accredited by Digi-Sign according to the criteria that Digi-Sign has set for the purpose of transfer of:

- Personal particulars to Digi-Sign in support of Subscriber applications for Personal ID-Cert Class 1 pursuant to section 2.1 of this CPS; and
- Subscriber Application details to Digi-Sign in support of Subscriber applications for Organizational ID-Cert Class 2 pursuant to section 2.1 of this CPS.
- Subscriber Application details to Digi-Sign in support of Subscriber applications for Encipherment ID-Cert Class 3 pursuant to section 2.1 of this CPS.

**“Applicant”** means a natural or legal person who applies to Digi-Sign for an ID-Cert.

**“Arbitration”** refers to the process that Digi-Sign and its Subscribers have agreed to undertake that any dispute or difference arising from, or in connection with, the terms and conditions specified in the Subscriber Application form and this CPS will not be heard by a court but by a private individual or a panel of several private individuals.

**“Authorized Delegate”** in relations to Digi-Sign ID-Cert Class 2 or Class 3 refers to a person who has been authorized by his organization to apply and make use of a Digi-Sign ID-Cert Class 2 or Class 3 on behalf of the organization.

**“Certificate” or “ID-Cert”** means a record which:

- a) is issued by Digi-Sign in its role as a Recognized Certification Authority for the purpose of supporting a digital signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair;
- b) identifies Digi-Sign in its role as a Recognized Certification Authority issuing it;
- c) names or identifies the person to whom it is issued;
- d) contains the public key of the person to whom it is issued; and
- e) is signed by a responsible officer of Digi-Sign issuing it.

**“Certification Authority”** refers to Digi-Sign in its role of issuing ID-Cert to a person or organization (who may be another certification authority).

**“Certification Practice Statement (CPS)”** refers to a statement issued by Digi-Sign to specify the practices and standards that Digi-Sign employs in issuing ID-Cert as from time to time amended or revised.



**“Certificate Revocation List (CRL)”** A data structure that enumerates public-key certificates (or other kinds of certificates) that have been invalidated by Digi-Sign prior to the time at which the ID-Cert were scheduled to expire.

**“Correspond”** in relation to private or public keys, means to belong to the same key pair.

**“Cryptosystem”** means a system capable of generating a secure key pair, consisting of a private key for generating a digital signature and a public key to verify the digital signature.

**“Digital Signature”** in relation to an electronic record, means an electronic signature of the signor generated by the transformation of the electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can determine:-

- a) whether the transformation was generated using the private key that corresponds to the signer's public key; and
- b) whether the initial electronic record has been altered since the transformation was generated.

**“Electronic Record”** means a record generated in digital form by an information system, which can be:

- a) transmitted within an information system or from one information system to another; and
- b) stored in an information system or other medium.

**“Electronic Signature”** means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted for the purpose of authenticating or approving the electronic record.

**“Information”** includes processed data, text, images, sound, computer programs, software and databases.

**“Information System”** means a system which:

- a) processes information;
- b) records information;
- c) can be used to cause information to be recorded, stored or otherwise processed in other information systems (wherever situated); and
- d) can be used to retrieve information, whether the information is recorded or stored in the system itself or in other information systems (wherever situated).

**“Intermediary”** in relation to a particular electronic record, means a person who on behalf of a person, sends, receives or stores that electronic record or provides other incidental services with respect to that electronic record.

**“Issue”** in relation to an ID-Cert, means the act of Digi-Sign of creating the ID-Cert and notifying its contents to the person or organization named in that ID-Cert.



**“Key Pair”**, in an asymmetric cryptosystem, key pair means a private key and its mathematically related public key, where the public key can verify a digital signature that the private key generates.

**“Mediation”** involves the appointment of a third party to assist Digi-Sign and its Subscribers to reach a settlement of their differences arising from, or in connection with, the terms and conditions specified in the Subscriber Application form, or this CPS; the mediator is not given the power to impose a settlement, but his power is to break any impasse and encourage the parties to reach an amicable settlement.

**“Originator”** in relation to an electronic record, means a person, by whom, or on whose behalf, the electronic record is sent or generated but does not include an intermediary.

**“Private Key”** means the key of a key pair used to generate a digital signature.

**“Public Key”** means the key of a key pair used to verify a digital signature.

**“Recognized Certificate”** means:

- a) a certificate recognized under Section 22 of Electronic Transactions Ordinance; or
- b) a certificate of a type, class or description of certificate recognized under Section 22 of Electronic Transactions Ordinance.

**“Recognized Certification Authority”** means a certification authority recognized under section 21 of Electronic Transactions Ordinance.

**“Record”** means information that is inscribed on, stored in or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in a perceivable form.

**“Reliance Limit”** means the monetary limit specified for reliance on an ID-Cert issued by Digi-Sign.

**“Repository”** means an information system for storing and retrieving certificates and other information relevant to Digi-Sign ID-Cert and Subscribers, CRL, CPS, and any other information that Digi-Sign may publish from time to time.

**“Responsible Officer”** in relation to a Recognized Certification Authority, means an employee of Digi-Sign occupying a position of responsibility in relation to the activities in the Digi-Sign certification services relevant to the Electronic Transactions Ordinance.

**“Sign”** and **“Signature”** include any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating or approving a record.

**“Subscriber”** means a person or organization who has signed a Subscriber Application form and read the corresponding terms and conditions and who:

- a) is named or identified in an ID-Cert as the person or organization to whom the ID-Cert is issued;



- b) has accepted that ID-Cert;
- c) holds a private key which corresponds to a public key listed in that ID-Cert; and
- d) qualifies as a Subscriber under this CPS.

**“Subscriber Application”** means an application request from an Applicant who applies to Digi-Sign for an ID-Cert.

**“Trustworthy System”** means the Digi-Sign computer hardware, software and procedures that:

- a) are reasonably secure from intrusion and misuse;
- b) are at a reasonable level in respect of availability, reliability and ensuring a correct mode of operations for a reasonable period of time;
- c) are reasonably suitable for performing their intended function; and
- d) adhere to generally accepted security principles.

**“Verify a Digital Signature”** in relation to a given digital signature, electronic record and public key, means to determine that:

- a) the digital signature was generated using the private key corresponding to the public key listed in a certificate; and
- b) the electronic record has not been altered since its digital signature was generated, and any reference to a digital signature being verifiable is to be construed accordingly.

For the purpose of the Electronic Transactions Ordinance, a digital signature is taken to be supported by a certificate if the digital signature is verifiable with reference to the public key listed in a certificate the Subscriber of which is the signer.

## Appendix 1

### Digi-Sign Certification Services Limited ID-Cert Profile

#### 1. Personal ID-Cert Class 1: Certificate Specification

Description: This class of certificate is issued to individuals for authentication purpose. Such individuals may include holders of Hong Kong ID cards, and holders of passport or other travel document indicating that the holder's limit of stay in Hong Kong has not expired.

Field	Content	Remarks
<b>Basic Certificate Fields</b>		
<b>Version</b>	X.509 V3	
<b>Serial Number</b>	[Assigned by CA]	
<b>Signature Algorithm ID</b>	SHA1withRSAEncryption	
<b>Issuer</b>	C=HK O=DIGI-SIGN CERTIFICATION SERVICES LIMITED OU=BRN 31346952-000 CN=ID-CERT SIGNING CA CERT	OU stores the Hong Kong Business Registration Number of Digi-Sign.
<b>Validity</b>		The validity period is 2 years.
<b>Not Before</b>	[Issue date set by CA]	UTC Time
<b>Not After</b>	[Expiry date set by CA]	UTC Time
<b>Subject</b>	C=HK O=DS ID-CERT CLASS 1 ([Certificate Request Number assigned by CA]) OU=[Subscriber Number assigned by CA] CN=[Name of individual as printed on HKID card or passport or other travel document]	
<b>Subject Public Key Information</b>		
<b>Cryptographic Algorithm ID</b>	RSA (1024 bit)	
<b>Public Key</b>	[Bound by CA]	
<b>Issuer Unique Identifier</b>		Not used.
<b>Subject Unique Identifier</b>		Not used.
<b>CA Signature Algorithm ID</b>	SHA1withRSAEncryption	It is the same as the Signature Algorithm ID.
<b>CA Signature</b>	[Produced by CA]	
<b>Standard Certificate Extensions</b>		
<b>Authority Key Identifier</b>		
<b>Public Key Identifier</b>	[Set as the Subject Key Identifier of the CA certificate used to sign this certificate]	
<b>Issuer Serial Number</b>		Not used.
<b>Subject Key Identifier</b>	[Set based on the Subject's public key bound to this certificate]	
<b>Key Usage</b>	Digital signature, Non-repudiation	
<b>Certificate Policies</b>		
<b>Policy OID</b>	1.3.6.1.4.1.8420.1	
<b>CPS URL</b>	<a href="http://www.dg-sign.com">www.dg-sign.com</a>	
<b>User Notice</b>		Not used.



<b>Subject Alternative Name</b>		
<b>Email Address</b>	[Email address provided by Subscriber]	
<b>DNS Name</b>	[Encoded Subscriber ID]	The encoding formula of the Subscriber ID is : Sha1[RSASha1[Subscriber ID]] where Subscriber ID = HKID or passport or other travel document number of the individual.
<b>Basic Constraints</b>		
<b>Subject Type</b>	End entity.	
<b>Path Length Constraint</b>	None.	
<b>Netscape Extensions</b>		
<b>Netscape Cert Type</b>	SSL Client, S/MIME Client	
<b>Netscape Comment</b>		Not used.
<b>Netscape SSL Server Name</b>		Not used.
<b>Other Extensions</b>		
<b>Foreign ID Indicator</b>	[Set as "P" in ASN.1 Octet String]	This extension will appear only if the Subscriber provides non HKID identity document to substantiate their identity in applying for the certificate.



## 2. Organizational ID-Cert Class 2: Certificate Specification

Description: This class of certificate is issued to organizations for authentication purpose. Such organizations must be registered in the Hong Kong Special Administrative Region.

Field	Content	Remarks
<b>Basic Certificate Fields</b>		
<b>Version</b>	X.509 V3	
<b>Serial Number</b>	[Assigned by CA]	
<b>Signature Algorithm ID</b>	SHA1withRSAEncryption	
<b>Issuer</b>	C=HK O=DIGI-SIGN CERTIFICATION SERVICES LIMITED OU=BRN 31346952-000 CN=ID-CERT SIGNING CA CERT	OU stores the Hong Kong Business Registration Number of Digi-Sign.
<b>Validity</b>		The validity period is 2 years.
<b>Not Before</b>	[Issue date set by CA]	UTC Time
<b>Not After</b>	[Expiry date set by CA]	UTC Time
<b>Subject</b>	C=HK O=DS ID-CERT CLASS 2 ([Certificate Request Number assigned by CA]) OU=[Name of the registered organization] and [Registration number of the organization] and [Subscriber Number assigned by CA] CN=[Name of the authorized delegate of the organization]	Registration number of the organization would follow the following convention: a) BRN 99999999-999 : Business Registration Number b) CI 99999999 : Certificate of Incorporation c) CR 99999999 : Certificate of Registration d) OTH X(30) : Country Code (where the organization is incorporated in) and other identification, maximum 30 char, can be blank if the organization is incorporated in the Hong Kong SAR
<b>Subject Public Key Information</b>		
<b>Cryptographic Algorithm ID</b>	RSA (1024 bit)	
<b>Public Key</b>	[Bound by CA]	
<b>Issuer Unique Identifier</b>		Not used.
<b>Subject Unique Identifier</b>		Not used.
<b>CA Signature Algorithm ID</b>	SHA1withRSAEncryption	It is the same as the Signature Algorithm ID.
<b>CA Signature</b>	[Produced by CA]	
<b>Standard Certificate Extensions</b>		
<b>Authority Key Identifier</b>		
<b>Public Key Identifier</b>	[Set as the Subject Key Identifier of the CA certificate used to sign this certificate]	
<b>Issuer</b>		Not used.
<b>Serial Number</b>		Not used.
<b>Subject Key Identifier</b>	[Set based on the Subject's public key bound to this certificate]	
<b>Key Usage</b>	Digital signature, Non-repudiation	
<b>Certificate Policies</b>		
<b>Policy OID</b>	1.3.6.1.4.1.8420.1	
<b>CPS URL</b>	<a href="http://www.dg-sign.com">www.dg-sign.com</a>	



Digi-Sign Certification Practice Statement

<b>User Notice</b>		Not used
<b>Subject Alternative Name</b>		
<b>Email Address</b>	[Email address provided by Subscriber]	
<b>DNS Name</b>	[Encoded Subscriber ID]	The encoding formula of the Subscriber ID is : Sha1[RSASha1[Subscriber ID]] where Subscriber ID = Registration number of the organization.
<b>Basic Constraints</b>		
<b>Subject Type</b>	End entity.	
<b>Path Length Constraint</b>	None.	
<b>Netscape Extensions</b>		
<b>Netscape Cert Type</b>	SSL Client, S/MIME Client	
<b>Netscape Comment</b>		Not used.
<b>Netscape SSL Server Name</b>		Not used.



### 3. Encipherment ID-Cert Class 3 Certificate Specification

Description: This class of certificate is issued to individuals and organizations for encryption and decryption of electronic messages and acknowledgment of receipt of encrypted messages.

Field	Content	Remarks
<b>Basic Certificate Fields</b>		
Version	X.509 V3	
Serial Number	[Assigned by CA]	
Signature Algorithm ID	SHA1withRSAEncryption	
Issuer	C=HK O=DIGI-SIGN CERTIFICATION SERVICES LIMITED OU=BRN 31346952-000 CN=ID-CERT SIGNING CA CERT	OU stores the Hong Kong Business Registration Number of Digi-Sign.
Validity		The validity period is 2 years.
Not Before	[Issue date set by CA]	UTC Time
Not After	[Expiry date set by CA]	UTC Time
Subject	C=HK O=DS ID-CERT CLASS 3 ([Certificate Request Number assigned by CA]) OU=[Name of the individual as printed in HKID or passport or other travel document] – in the case of an individual being the applicant [Name of the registered organization] – in the case of an organization being the applicant and [Subscriber Number assigned by CA] CN=[Email address provided by Subscriber]	
Subject Public Key Information		
Cryptographic Algorithm ID	RSA (1024 bit)	
Public Key	[Bound by CA]	
Issuer Unique Identifier		Not used.
Subject Unique Identifier		Not used.
CA Signature Algorithm ID	SHA1withRSAEncryption	It is the same as the Signature Algorithm ID.
CA Signature	[Produced by CA]	
<b>Standard Certificate Extensions</b>		
Authority Key Identifier		
Public Key Identifier	[Set as the Subject Key Identifier of the CA certificate used to sign this certificate]	
Issuer		Not used.
Serial Number		Not used.
Subject Key Identifier	[Set based on the Subject's public key bound to this certificate]	
Key Usage	Digital signature, Key encipherment	
Certificate Policies		
Policy OID	1.3.6.1.4.1.8420.1	
CPS URL	<a href="http://www.dg-sign.com">www.dg-sign.com</a>	
User Notice		Not used
Subject Alternative Name		



Digi-Sign Certification Practice Statement

<b>Email Address</b>	[Email address provided by Subscriber]	
<b>DNS Name</b>		Not used
<b>Basic Constraints</b>		
<b>Subject Type</b>	End entity.	
<b>Path Length Constraint</b>	None.	
<b>Netscape Extensions</b>		
<b>Netscape Cert Type</b>	SSL Client, S/MIME Client	
<b>Netscape Comment</b>		Not used.
<b>Netscape SSL Server Name</b>		Not used.



## Appendix 2

**Digi-Sign Certification Services Limited  
ID-Cert CRL Specification**

Field	Content	Remarks
<b>Version</b>	X.509 V2	
<b>Signature Algorithm ID</b>	SHA1withRSAEncryption	
<b>Issuer</b>	C=HK O=DIGI-SIGN CERTIFICATION SERVICES LIMITED OU=BRN 31346952-000 CN=ID-CERT SIGNING CA CERT	OU stores the Hong Kong Business Registration Number of Digi-Sign.
<b>This Update</b>	[Set by CA]	UTC Time
<b>Next Update</b>	[Set by CA]	UTC Time
<b>Revoked Certificates</b>		
<b>User Certificate</b>	[Certificate serial number set by CA]	
<b>Revocation Date</b>	[Set by CA]	
<b>CRL Entry Extension</b>		
<b>Reason Code</b>	[Set by CA]	
<b>CRL Extensions</b>		
<b>Authority Key Identifier</b>		
<b>Public Key Identifier</b>	[Set as the Subject Key Identifier of the CA used to sign this CRL]	
<b>Issuer</b>		Not used.
<b>Serial Number</b>		Not used.
<b>CRL Number</b>	[Set by CA]	
<b>CA Signature Algorithm ID</b>	SHA1withRSAEncryption	It is the same as the Signature Algorithm ID.
<b>CA Signature</b>	[Produced by CA]	



**Appendix 3****Digi-Sign Certification Services Limited****Key and Certificate Life Cycle Management Plan**

The Digi-Sign keys and certificates have a predetermined life span. Digi-Sign has set its key and certificate life cycle management plan as below:

**Current Life Cycle**

<b>Types</b>	<b>Start Date</b>	<b>Expiry Date</b>	<b>Rollover Instructions</b>
Root CA	24.7.2001	22.7.2011	Rollover of key pair and certificate must be completed on or before 1.6.2009
Sub CA	24.7.2001	21.7.2011	Rollover of key pair and certificate must be completed on or before 2.6.2009
Subscribers: (1) Issue on 1 <sup>st</sup> day  (2) Issue after 1 <sup>st</sup> day & replacement	(1) 25.7.2001  (2) 26.7.2001 & thereafter, but must not extend beyond 15.6.2009	(1) 24.7.2003  (2) 25.7.2003 & thereafter, as extended by 2 years from start date, and the latest expiry date must be 14.6.2011	Rollover is not applicable to Subscriber keys and ID-Cert

**Next Life Cycle**

<b>Types</b>	<b>Start Date</b>	<b>Expiry Date</b>	<b>Rollover Instructions</b>
Root CA	2.6.2009	1.6.2019	Rollover of key pair and certificate must be completed on or before 15.4.2017
Sub CA	2.6.2009	31.5.2019	Rollover of key pair and certificate must be completed on or before 16.4.2017
Subscribers: (3) Further issue & replacement	(3) 16.6.2009 & thereafter, but must not extend beyond 30.4.2017	(3) 15.6.2011 & thereafter, as extended by 2 years from start date, and the latest expiry date must be 29.4.2019	Rollover is not applicable to Subscriber keys and ID-Cert

