Digi-Sign Certification Services Limited

Certification Practice Statement

OID: 1.3.6.1.4.1.8420.4.1.2

In support of the Digi-Sign "General Purpose" CA Hierarchy

Dec 2005

Table of Contents

1 INTRODUCTION

Section 1: Introduction: This section identifies and introduces the CPS provisions, and indicates the types of entities and applications for which the CPS is targeted.

1.1. Overview

This Certification Practice Statement (CPS) is known as the Digi-Sign "General Purpose" CPS. It describes the practices and procedures involved in the issuance of public key digital certificates by Digi-Sign' s "General Purpose" PKI hierarchy.

1.1.1. Recognized and General Purpose Certificate

Under the Electronic Transactions Ordinance (Cap. 553), a Certification Authority may apply to the Government Chief Information Officer ("GCIO") to become a Recognized Certification Authority.

The recognition status is intended to give consumers confidence in using digital certificates issued by a Recognized Certification Authority, thus promoting the wider use of electronic transactions in the community. Recognition shall only be granted to those Certification Authorities that have achieved a standard acceptable to the Government of the Hong Kong Special Administrative Region (HKSAR).

Recognition imposes a high standard of assurance on the subject CA. As a recognized CA, Digi-Sign must comply with the *Code of Practice for Recognized Certification Authorities* and be regularly audited. The use of digital certificates by Subscribers and Relying Parties conveys significant benefits, in particular, if a rule of law requires the signature of a person or provides for certain consequences if a document is not signed by a person. For government related transactions, a digital signature of the person satisfies the requirement for signature if the digital signature is supported by a recognized certificate and is generated within the validity of that certificate. For transactions not involving government entities, a digital signature of the person satisfies the requirement for signature if the digital signature is generated by a reliable and appropriate means and agreed by the recipient of the signature within the validity of that certificate.

1.2. Policy Identification

1.2.1. Certificate Policy (CP) Identification

1.3	ISO assigned / ISO identified organisation

6.1.4.1	Internet related IANA registered private enterprise
8420	Digi-Sign Certification Services Limited
4 (example)	Document number
1.0 (example)	Version number

1.2.2. CPS Identification

This CPS has been allocated the OID: 1.3.6.1.4.1.8420.4.1.2

The CPS is published on a Digi-Sign website, as follows: http://www.dg-sign.com.

Certificates supported by this CPS may contain the Uniform Resource Identifier (URI) of the CPS in the CPS pointer qualifier field of the *Certificate Polices* extension (i.e. www.dg-sign.com).

1.3. Community and Applicability

This CPS is applicable to:

- the Digi-Sign "General Purpose" Certification Authority(s)
- any subordinate Registration Authority (RA) within the Digi-Sign "general purpose" hierarchy
- Subscribers registered for Digi-Sign "general purpose" keys and certificates.

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

Refer to the applicable CP.

1.3.1. Policy Approval Authority

The practices and procedures in this CPS are approved and published by a Policy Approval Authority (PAA). The Digi-Sign Management Committee (Digi-Sign Senior Managers) act as the Digi-Sign PAA. The PAA maintains the integrity of the policy infrastructure for the Digi-Sign "General Purpose" PKI.

1.3.2. Certification Authority (CA)

The primary purpose of the CA is to provide certificates and certificate management services to Subscribers (certificate holders) or subordinate CAs within its certificate policy domains.

A CA can issue various CPs. Each CP is applicable to a particular community and/or class of applications with common security requirements. Each certificate issued by the CA is issued under a nominated CP.

1.3.3. Registration Authority (RA)

The Registration Authority (RA) is subordinate to the CA. The primary purpose of the RA is to receive and authenticate Subscriber certificate and revocation requests.

1.3.4. Subscribers

Subscribers may be individuals. Often Subscribers will be employees or customers of an organization that has entered into a contractual relationship for the provision by Digi-Sign of commercial CA services within a closed PKI model (the "sponsoring organization").

Subscribers may also be devices or applications.

Refer to the applicable CP.

1.3.5. Relying Parties

Only parties explicitly referenced in an associated Digi-Sign CP may rely on a certificate issued under this CPS. The Digi-Sign "General Purpose" PKI functions as a "closed model" PKI and does not generally support third party reliance. Where third party reliance is supported, it must be strictly controlled by contract and the limits to that reliance will also be clearly defined in the applicable CP. No third party stranger may ever rely on a certificate issued under this CPS.[1]

1.3.6. Applicability

Each CP published under this CPS must contain an *Applicability* section, clearly defining the general purpose of the relevant certificate type. Ideally the *Applicability* section contains details regarding:

- the general purpose of the certificate type and expected use
- any restrictions on use
- any applications and functions the certificate MUST NOT be used for.

In general, Digi-Sign certificates issued under this CPS are only to be used by organisations and individuals who have a current, documented contractual relationship with Digi-Sign. Certificates issued under this CPS must only be used with applications that:

- correctly establish, transfer and use the public and private keys
- are capable of performing the appropriate certificate validity and verification checking, and
- report appropriate information and warnings to the Subscriber and /or Relying Party.

[1] A "third party stranger" is a third party who does not have a contractual relationship with Digi-Sign which specifically entitles the third party to rely on Digi-Sign certificates of a particular type and class for a particular purpose.

1.4. Contact Details

This CPS is approved and published by the Digi-Sign PAA.

1.4.1. Contact Person

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

Address:
Digi-Sign Certification Services Limited

11/F & 12/F, Tower B, Regent Centre,
63 Wo Yip Hop Road, Kwai Chung,
Hong Kong

Digi-Sign Hotline Details:

Tel: (852) 2917 8833

Fax: (852) 2174 0019

Email: hotline@dg-sign.com

Other contact details:

Website: http://www.dg-sign.com

Repository: ldap1.dg-sign.com

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

Saturday 8:30am to 12:30pm

Emergency details:

In case a tropical cyclone warning signal no.8 (or above) or a black rainstorm warning signal is hoisted, Digi-Sign' s office will open at its usual hour if the signal is lowered at or before 6 a.m. on that day. If the signal is lowered between 6 a.m. and 10 a.m., Digi-Sign' s office will not open until 2:00 p.m. for any weekday other than Saturday, Sunday or Public Holiday. If the signal is hoisted or not lowered after 10:00a.m., Digi-Sign' s office will not open for the whole day.

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.

The contact person can provide copies of, or access to, the CP(s) and CPS and answer questions relating to the policy, practices and procedures described in these documents.

1.4.2. Person determining CPS suitability for this policy

The Digi-Sign PAA will determine whether this CPS provides suitable support for each individual CP applying within the Digi-Sign "General Purpose" PKI. The PAA will review both documents to ensure that the practices documented in the CPS fulfil the requirements defined in each CP.

1.5. Relationship between this CPS and associated Certificate Policies (CPs)

A unique CP is written to individually support each different type of certificate. A CP is a written document setting out the rights, duties and obligations of each party in a PKI. Typically, a CP is used to define and limit the use of certificates issued under that CP. A CPS, on the other hand, explains how the requirements of the CP are met in procedural and operational terms. One CPS may support a variety of CPs. (See Annex A for a list of CPs supported by this CPS). The table below highlights key differences between a CP and a CPS.

Certificate Policy (CP)	Certification Practice Statement (CPS)
What	How
Less specific	More detailed
Independent of specific implementation	Tailored to organizational structure, operating procedures, facilities and computing environment of a particular CA.
User defines	Provider defines
Requirements	Procedures

1.5.1. Hierarchy of documents

This CPS contains default provisions that are overridden by the contents of an applicable CP. In most cases the contents of the CPS and the CP are complementary, that is, some of the components set down by RFC2527 (see section 2.9.1) appear in the CPS and the remaining components appear in the applicable CP. However, in cases where both the CPS and the CP contain the same component, the CP will take precedence over the CPS.

A written service agreement, or other written contract between Digi-Sign and an affected party, will take precedence over the CP and the CPS.

2. GENERAL PROVISIONS

Section 2: General Provisions: This section specifies the applicable presumptions on a range of legal and general practices topics. The CPS sets out broad principles only. It must be considered in conjunction with Section 2 of the applicable Certificate Policy (CP) and any applicable Service Agreement or other written contract with Digi-Sign.

2.1 Obligations

The prime obligation for Digi-Sign is to use trustworthy systems that meet or exceed industry best practice standards for commercial Certification Authorities.

Typically, the responsibilities and liabilities of Digi-Sign and other parties are not listed comprehensively in a single section of any one document. Rather, these appear in the various sections of the CPS, the applicable CP and the applicable contracts, for example, the Subscriber Agreement or Subscriber Terms and Conditions. In particular, they will usually appear as covenants within sections 1.3 *Community and Applicability* and 2.1 *Obligations* of the applicable CP.

2.1.1. Root Certification Authority (RCA) Obligations

The Root CA accepts the following obligations:

- Comply with industry "best practice standards" for a commercial RCA and operate a trustworthy system
- Maintain the life cycle and protect the security of the RCA keys
- Notify subordinate CAs of the issuance of their certificate, including the timing of its issuance
- Issue the CA certificate to approved subordinate CAs
- Publish the list of certificates issued by the RCA under this CPS
- Publish a list of any subordinate CA certificates suspended or revoked, and notify any subordinate CA of the suspension or revocation, including the timing of such suspension or revocation.

2.1.2. Certification Authority (CA) Obligations

As the issuing CA, Digi-Sign accepts the following obligations:

- Comply with industry "best practice standards" for a commercial CA and operate a trustworthy system
- Publish this CPS and the related Certificate Policies 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 Subscribers of the issuance of their certificate, including the timing of its issuance
- For centrally generated Subscriber keys, issue the private key and certificate to the Subscriber

- For centrally generated Subscriber keys, protect the security of the private key before and during its delivery to the Subscriber
- For Subscriber generated keys, issue the correct corresponding certificate
- For Subscriber generated keys, use a trustworthy method to establish Subscriber possession of private key
- Publish the list of certificates issued under every supported CP and a list of Subscribers
- Publish a list of the certificates suspended or revoked.

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

2.1.3. Registration Authority (RA) Obligations

Refer to the applicable CP.

2.1.4. Subscriber Obligations

Refer to the applicable CP.

2.1.5. Repository Obligations

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

- Publish the certificates issued
- Regularly publish the Certificate Revocation List ("CRL")
- Publish the Authority Revocation List ("ARL"), and update this ARL promptly upon the suspension or revocation of a CA certificate
- Provide a means of access to the Digi-Sign repository by the Subscribers, relying parties, and others who may be interested in the certificates, or the public information regarding the Digi-Sign certification services
- Publish the current and prior versions of the CPS
- Publish the current and prior versions of the CP; and
- Maintain the accessibility to the repository, except when it is necessary to suspend this access for maintenance or related reason.

The Digi-Sign Repository may be accessed at: ldap1.dg-sign.com.

2.1.6. Relying Parties Obligations

Only parties explicitly referenced in an associated Digi-Sign CP may rely on a "General Purpose" Digi-Sign certificate. The Digi-Sign "General Purpose" PKI functions as a "closed model" PKI and does not generally support third party reliance. (See section 1.3.5 above). Where third party reliance is supported under an associated CP, relying parties must:

- abide by the terms and conditions of this CPS, the applicable CP and any relevant contractual agreement
- only use an associated certificate in accordance with the provisions of the applicable CP and strictly observe any restrictions or prohibitions on certificate use
- agree that no implied or express warranties are given by Digi-Sign or by any other entity who may be involved in the issuing or managing of key pairs and/or certificates and all statutory warranties are to the fullest extent permitted by law expressly excluded
- accept liability for any loss the relying party may suffer through failing to act within the reliance limits of a Digi-Sign certificate as indicated in the applicable CP
- check the certificate' s status and confirm the certificate has not been revoked
- verify and validate the certificate before use, including, at a minimum, a check of the following X.509 fields and extensions:
    - validity (*notBefore* & *notAfter*)
    - subject public key
    - key usage extension
    - certificate policies extension.

2.2. Liability

Limitations to the extent of the liability of involved parties are described in the applicable CP, the Subscriber Agreement or Subscriber Terms and Conditions, and any other relevant contractual documents.

In the absence of any documented contractual relationship between the CA and a Subscriber and/or relying party, Digi-Sign does not accept any liability regarding the operations of the Digi-Sign "General Purpose" PKI.

No implied or express warranties are given by Digi-Sign or by any other entity who may be involved in the issuing or managing of key pairs and/or certificates and all statutory warranties are to the fullest extent permitted by law expressly excluded.

2.3. Financial Responsibility

2.3.1. Indemnification of CA and/or RA

Refer to the applicable CP.

2.3.2. Fiduciyary Relationships

Issuing certificates under this CPS, or assisting in the issue of these certificates, does not make Digi-Sign an agent, fiduciary, trustee, or other representative of any Subscriber, Relying Party or other third party.

2.3.3. Administrative Processes

No stipulation.

2.4. Interpretation and Enforcement

Refer to the applicable CP.

2.5. Fees

Refer to the applicable CP.

2.6. Publication and Repositories

The Digi-Sign "General Purpose" PKI utilises an X.500 directory, providing access to certificates and CRLs for members of the Digi-Sign community. The directory is a repository for:

- active certificates (new and renewed)
- revoked Subscriber certificates (in the CRL)
- revoked CA certificates (in the ARL)
- expired certificates.

The Digi-Sign directory is available 24 hours a day, 7 days a week.

2.6.1. Publication of CA Information

CA certificates, and their corresponding hash values, are published to the directory at the time the CA certificate is generated. In addition, the hash values of the Root CA are published on a website, as follows: http://www.dg-sign.com

2.6.1.1. Publication of Policy and Practice Information

This CPS is published electronically at:http://www.dg-sign.com. Hard copies of this CPS are available from the contact person nominated at section 1.4.1 above upon request.

2.6.2. Frequency of Publication

2.6.2.1. Frequency of Certificate Publication

Certificates are usually published within 24 hours of generation. See CP.

2.6.2.2. Frequency of ARL/CRL Publication

While the certificate is revoked immediately after the CA processes the revocation request, any end user checking the validity of a certificate will not be able to detect the revocation until the next CRL posting.

The Root CA will publish an updated ARL as required.

The issuing CA will publish an updated CRL at least once every 24 hours.

2.6.3. Access Control

There are no access controls on the reading of this CPS or the associated CPs on the Digi-Sign website.

Access to Certificate information (including CRLs) within the directory is generally limited to a single name search enquiry using LDAP (although this may differ for implementations under HTTP).

Appropriate access controls are used to restrict to authorised personnel the ability to write to or modify these items.

2.7. Compliance Audit

The Digi-Sign "General Purpose" PKI is to be audited on a regular basis to assure compliance with industry best practice and other applicable standards that may apply from time to time.

2.7.1. Frequency of entity compliance audit

Internal auditing by the internal auditors will be continuous. External audits will be conducted at the discretion of the Digi-Sign PAA. Note that the Digi-Sign General Purpose PKI hierarchy is operated in the same manner as the Digi-Sign Recognized hierarchy, which is audited according to the *Code of Practice for Recognized Certification Authorities* on at least an annual basis.

2.7.2. Identity / qualifications of auditor

Auditors must have:

- a minimum of two (2) years auditing experience
- excellent understanding of an IT security environment
- excellent understanding of PKI technologies and operations.

2.7.3. Auditor' s relationship to audited party

Use of internal and external auditors is at the discretion of the Digi-Sign PAA.

2.7.4. Topics covered by audit

Topics covered by audit include:

- effective delivery of the Digi-Sign certification services
- adherence to privacy requirements
- adherence to key management requirements
- physical security controls
- storage and handling requirements of information

- logical security controls
- media management requirements
- configuration baseline management
- change management
- business continuity and disaster recovery plan
- incident management procedures
- risk management procedures
- adherence to personnel security control requirements
- implementation of internal systems verification programmes.

2.7.5. Actions taken as a result of deficiency

An audit report detailing all of the audit findings will be completed and issued after the audit' s closing meeting. The report includes details on any issue and/or recommendation raised as a result of the information obtained during the course of the audit. A follow-up audit may then be undertaken in order to review completion of the actions/issues /discrepancies identified during the closing meeting of a previous audit.

2.7.6. Communication of results

Audit reports from internal audits will be forwarded to the Digi-Sign PAA. The auditor shall not disclose any of the audit findings, or information with respect to the Digi-Sign "General Purpose" PKI operations to any other party unless the Digi-Sign PAA formally approves that disclosure. All information collected during the course of the audit must be treated as confidential unless otherwise advised by the PAA.

2.8. Confidentiality

The Digi-Sign Privacy Policy is available on the Digi-Sign website.

2.9. Intellectual Property Rights

All intellectual property rights in documents, electronic or otherwise, published by the Digi-Sign PAA belong to and will remain the property of Digi-Sign.

2.9.1. Attribution

The use of these documents in the preparation of this CPS is gratefully acknowledged:

- Chokhani and Ford, *RFC2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, 1999 (©The Internet Society 1999), and
- American Bar Association, *PKI Assessment Guidelines: Public Draft for Comment*, v0.30 (©American Bar Association 2001).

3. IDENTIFICATION AND AUTHENTICATION

Section 3: Identification and Authentication: This section describes the procedures used to authenticate a certificate applicant to a CA or RA prior to certificate issuance. It also describes how parties requesting re-key or revocation are authenticated. Section 3 also addresses naming practices, including name ownership recognition and name dispute resolution. Section 3 of the CPS is very general and must be considered in conjunction with the relevant sections of the applicable CP and any applicable Service Agreement or other written contract with Digi-Sign.

3.1. Initial Registration

3.1.1. Types of names

In general, certificates will contain the name of the Subscriber in the X.509 certificate field *SubjectName*. This field must be a unique identifier of the subject and will contain a standards-based Distinguished Name (DN). Detailed information regarding name forms is contained in the applicable CP.

3.1.2. Need for names to be meaningful

In general, names used within Digi-Sign "general purpose" certificates are intended to indicate a binding between a public key and a real-world identity. Anonymous or pseudonymous certificates are not supported.

3.1.3. Rules for interpreting various name forms

In general, certificates will use standards-based distinguished names that are readily distinguishable and do not require special interpretive rules.

Note that the presence of any organizational or employment related information in a Subscriber' s certificate or directory entry does not necessarily indicate authority to act on behalf of that organization or to bind the organization. Relying parties must always consult the applicable CP in order to determine the limits of reliance and must take steps to verify and validate the authority of the certificate subject to represent the organization in any specific transaction.

3.1.4. Uniqueness of names

Names must be unambiguous and unique.

3.1.5. Name claim dispute resolution procedure

Any dispute regarding competing claims to a Distinguished Name is to be resolved in terms of the Dispute Resolution Procedures indicated in the applicable CP.

3.1.6. Recognition, authentication and role of trademarks

Trademark rights or other IP rights are unlikely to exist in personal names used within certificates. However, under this CPS, Subscribers:

- authorise the issuing CA and its subordinate entities to use the relevant Intellectual Property for the purpose of creating a Distinguished Name and for other purposes reasonably necessary in relation to issue of Keys and Certificates
- warrant they are entitled to use that Intellectual Property for the purposes for which Keys and Certificates are issued; and
- agree to indemnify the issuing CA and its subordinate entities against loss, damage, costs or expenses of any kind (including legal costs on a solicitor-client basis) incurred by them in relation to any claim, suit or demand in respect of an infringement or alleged infringement of the IP rights of any person.

3.1.7. Method to prove possession of private key

Refer to the applicable CP.

3.1.8. Authentication of organisation identity

Refer to the applicable CP.

3.1.9. Authentication of individual identity

Refer to the applicable CP.

3.2. Certificate Renewal

See the applicable CP.

3.3. Renewal after Revocation

In general, rekey is not permitted after certificate revocation. Subscribers requiring a replacement certificate after revocation must apply for a new certificate, complying with all initial registration procedures and requirements as though they were a new user. See the applicable CP

3.4. Revocation Request

Revocation of a certificate is usually a permanent and irreversible event, meaning that the certificate cannot be used again. See the applicable CP.

4. OPERATIONAL REQUIREMENTS

Section 4: Operational Requirements: This section specifies requirements imposed upon issuing CA, subject CAs, RAs, or end entities with respect to various operational activities. As this section is concerned with operational detail, most of the relevant material is contained within this CPS.

4.1. Certificate Application

In general, it is not permitted to register a person without their consent (see the applicable CP). Digi-Sign reserves its absolute right to change the procedures to process the Subscriber Application from time to time without notice.

Upon submitting an application, the applicant warrants to Digi-Sign and any other entity who may be involved in the issuing or managing of key pairs and/or certificates that the information provided is true and correct, and must provide further proof to substantiate this information upon request.

4.2. Certificate Issuance

In order to issue a Digi-Sign "general purpose" certificate, the issuing CA constructs and populates the fields of an X.509 version 3 certificate, according to the requirements of the applicable CP and this CPS. The certificate is then signed with the CA's private authentication key. The certificate profile is usually defined within the applicable CP.

4.3. Certificate Acceptance

Generally, a Subscriber's receipt of a certificate, and their subsequent use of their keys and certificates, constitutes certificate acceptance. By accepting a certificate, the Subscriber:

- agrees to be bound by the continuing responsibilities, obligations and duties imposed on them by the Subscriber Agreement or Subscriber Terms and Conditions, the applicable CP and this CPS
- warrants that to their knowledge no unauthorised person has had access to the private key associated with the certificate
- asserts that the certificate information they have supplied during their registration interview is truthful and has been accurately and fully published within the certificate
- agrees that Digi-Sign has the authority to display the certificate in the repository
- undertakes to inform Digi-Sign immediately if the information supplied by the Subscriber at time of registration changes.

In some cases acceptance is signified when the Subscriber signs a letter of acceptance. Refer to the applicable CP.

4.4. Certificate Suspension and Revocation

4.4.1. Circumstances for revocation

Reasons for revoking a certificate include, but are not limited to:

- the theft, loss, disclosure, modification, or other compromise or suspected compromise of the Subscriber' s private key
- the misuse of keys and/or certificate(s) by the Subscriber
- the non-observance of the requirements in the Subscriber Agreement or Subscriber Terms and Conditions
- if the certificate information becomes or is found to be inaccurate
- if the Subscriber leaves the employment of the sponsoring organisation.

4.4.2. Who can request revocation

Before revoking a certificate, the issuing CA must obtain reliable evidence of the identity of the party initiating the revocation request. The following parties are usually authorised to request revocation of a Digi-Sign "general purpose" certificate:

- the issuing CA
- the RA who registered the Subscriber
- the Subscriber
- an authorised member of the Digi-Sign PKI operations staff
- an authorised employee of the sponsoring organisation.

Following revocation, the revoking CA posts the revoked certificate to the CRL.

There is no obligation to inform the Subscriber of the reason for revocation.

4.4.3. Procedure for revocation request

Refer to applicable CP.

4.4.4. Revocation request grace period

Revocation requests are verified on receipt and are usually actioned within 24 hours.

4.4.5. Circumstances for suspension

Suspension not supported.

4.4.6. Who can request suspension

Suspension not supported.

4.4.7. Procedure for suspension request

Suspension not supported.

4.4.8. Limits on suspension period

Suspension not supported.

4.4.9. CRL issuance frequency

Refer to the applicable CP.

4.4.10. Certificate status checking requirements

All relying parties MUST check the status of a certificate each time they use the certificate.

4.4.11. On-line revocation/status checking availability

Not applicable.

4.4.12. On-line revocation checking requirements

Not applicable.

4.4.13. Other forms of revocation advertisments available

Not applicable.

4.4.14. Checking requirements for other forms of revocation advertisments

Not applicable.

4.4.15. Special requirements in case of key compromise

Revocations performed for reasons of key compromise are performed according to the standard revocation procedures.

4.5. Security Audit Procedures

All operations of the Digi-Sign "general purpose" CAs and RAs are monitored, recorded and audited. See section 2.7 above, and the Digi-Sign *Information Security Guidelines and Practices* for more detailed information.

4.5.1. Types of event recorded

Digi-Sign will maintain an adequately comprehensive record of events relating to its daily PKI operations including, but not limited to:

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

4.5.2. Frequency of processing log

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

4.5.3. Retention period for audit 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.

4.5.4. Protection of audit log

As per the Digi-Sign *Information Security Guidelines and Practices.*

4.5.5. Audit log backup procedures

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

4.5.6. Audit collection system

The Digi-Sign PKI audit collection system combines automated and manual processes. The CA/RA software and/or the operating system automatically collect:

- Successful and failed attempts to:
    - Login and logoff

- Change operating system security parameters
- Create, modify or delete system accounts
- Create, modify or delete authorized system users
- Request, generate, sign, issue or revoke keys and certificates
- Create, modify or delete certificate holder information

- Application startup and shutdown
- Backup, archiving and restoration.

The operations personnel manually collect/record:

- Backup, archiving and restoration
- Systems configuration changes
- Software and hardware updates
- System maintenance
- Personnel changes.

4.5.7. Notification to event-causing subject

Notification procedures are set out in the Digi-Sign *Information Security Guidelines and Practices.* Notification of Subscribers and relying parties, other than where expressly described in this CPS or an applicable CP is at the discretion of Digi-Sign.

4.5.8. Vulnerability assessments

The entire Digi-Sign PKI is regularly subject to a comprehensive threat and risk assessment.

4.6. Records Archival

4.6.1. Types of event recorded

The following information is archived by the Digi-Sign PKI:

- application software such as the CA software
- databases
- CA and RA keys and activation data
- audit logs
- certificate request information
- certificates generated

- CRLs generated
- CA key rollover records
- complete back up registers
- copies of e-mail logs
- CPS
- CP
- contracts and formal correspondence, for example Letters of Acceptance where applicable
- operating procedures and manuals.

4.6.2. Retention period for archive

Certificates and archive information, including contracts, user records, certificates, CRLs, transaction records, audit logs and copies of the CP and CPS, are archived for a period of seven years from the date of expiry, unless another period is specifically required. There will be audit trails, which may be deemed to be sufficient for tracking of archival records.

4.6.3. 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.

4.6.4. Archive backup procedures

Digi-Sign has established archive back up procedures to ensure and enable complete restoration of current service in the event of a disaster. Any material held in off-site archive for backup purposes must be periodically tested to ensure that information is retrievable in the event of a failure. Material stored in off-site archive to meet legislative retention requirements need not be tested. 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.

4.6.5. Requirements for time-stamping of records

All automatically generated logs are time-stamped using the system clock of the computer on which they were generated. Manually generated records record the date of occurrence, but generally not the time.

4.6.6. Archive collection system (internal or external)

Archiving is performed by the Digi-Sign operations staff delegated with the responsibility for doing so.

4.6.7. Procedures to obtain and verify archive information

The integrity of the archives is verified:

- at any time when a full security audit is required
- at the time that the archive has been prepared.

4.7. Key Changeover

All CAs within the Digi-Sign "general purpose" hierarchy must notify their user community promptly, prior to the expiry of the CA keys and certificates. Subscriber certificates will typically have a shorter life span than the certificate of the issuing CA. Likewise, a subordinate CA certificate should have a shorter lifespan than the certificate of its issuing CA (e.g. the Root CA).

Digi-Sign has established an appropriate management framework and procedures to securely manage its CA keys, covering the keys for the Root CA, any sub CAs, CA Operators, Registration Authority and Registration Authority Operator. A specific document sets out the Digi-Sign CA Key Management Procedures.

4.7.1. Key changeover and archiving

Digi-Sign will keep the original CA keys in safe custody for a minimum of seven years subsequent to their respective expiry dates.

4.8. Compromise and Disaster Recovery

Digi-Sign maintains detailed documentation covering disaster recovery, business continuity and backup, archiving and offsite storage. These plans will be made available to those persons responsible for conducting a security audit. (They may also be made available to other interested parties at the discretion of Digi-Sign).

4.8.1. Computing resources, software and/or data are corrupted

The Digi-Sign documentation and/or the relevant technical manuals provide directions for identifying component failures, and managing subsequent service restoration. In the event of a system failure:

- the Security Officer or the Systems & Infrastructure Manager must be notified immediately
- the Security Officer or the Systems & Infrastructure Manager must authorise and oversee reloading of the appropriate ghost image and/or keys onto the applicable machine(s).

4.8.2. Entity key is compromised

The compromise of a private key is the most significant risk to PKI operations. Comprehensive procedures exist for dealing with such an event within Digi-Sign.

In the event of actual or suspected compromise of a Subscriber' s private key, the Subscriber must immediately notify Digi-Sign of the compromise. The Subscriber' s certificate will be promptly revoked.

In the event of actual or suspected compromise of a CA' s private key, the CA will immediately notify the rest of the affected hierarchy, including all subordinate entities within the CA' s chain of trust.

Responsibility for ensuring that key compromise actions are carried out promptly rests with the Security Officer and/or the Systems & Infrastructure Manager.

4.8.3. Business Continuity

Digi-Sign has taken adequate measures to provide resilience and redundancy for critical PKI components. Plans exist addressing the actions to be taken in order to restore core business operations as quickly as practicable when system operations have been significantly and adversely impacted by fire, strikes, etc.

Any staff member who becomes aware of or suspects a disruption or incident must report that disruption / incident to the Security Officer as soon as reasonably possible. The following are the actions to be taken if and when a disruption occurs:

- Identify the disruption
- Identify the critical functions and supporting resources impacted
- Assess the potential outage time for each critical function and resource
- Determine the applicable business continuity response or according to the arrangements
- Invoke additional disaster recovery measures, where necessary
- Inform the parties identified in the Plan as to the nature of the disruption, the potential outage time and remedial actions to be undertaken
- Where necessary, inform other affected parties such as Subscribers
- Track recovery progress, and determine whether any other remedial measures must be implemented
- Inform all affected parties when the disruption has been remedied and normal operations have resumed.

4.9. CA Termination

Digi-Sign has established appropriate procedures to deal with any need to withdraw its certification services and transfer its responsibilities as a Certification Authority to another entity - the Digi-Sign Termination Plan.

Digi-Sign will ensure the continued maintenance of records throughout the period of termination, and for any statutory period of retention required thereafter.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

Section 5: Physical, Procedural and Personnel Security Controls: This section describes the three main areas of non-technical security controls (that is, physical, procedural, and personnel controls) used by the issuing CA to perform securely the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

5.1. Physical Security Controls

Physical security controls generally meet or exceed the standards set in:

- *Information Security Management Standard BS 7799: 1999*
- *Code of Practice for Recognized Certification Authorities.*

5.1.1. Site Location and Construction

The Digi-Sign offices have been specifically fitted out for commercial certification services provision. The physical layout has been documented and a risk treatment strategy and physical security plan implemented.

5.1.2. Physical Access

Physical access is controlled and restricted according to trusted roles and need-to-know principles. Access is controlled electronically and manually, and is monitored for unauthorized entry and intrusion at all times.

5.1.3. Power and Air Conditioning

The Digi-Sign offices and operations centre are serviced by a standard power supply and air conditioning. All critical components are connected to uninterruptible power supply (UPS) units, to prevent abnormal shutdown in the event of a power failure. There is a dedicated air conditioning system that controls temperature and humidity.

5.1.4. Water Exposures

The Digi-Sign offices and operations centre are protected against water exposure by being located on an above ground floor of a building that is not in a flood zone.

5.1.5. Fire Prevention and Protection

The Digi-Sign offices and operations centre are subject to normal commercial fire prevention and protection procedures, including the installation of fire fighting equipment and smoke detectors.

5.1.6. Media Storage

All magnetic media containing sensitive Digi-Sign information, including backup media, are stored in containers, cabinets or safes with fire protection capabilities which are located either within the secure operating area or in a secure off-site storage area.

5.1.7. Waste Disposal

Removal of hardware components from Digi-Sign for servicing or disposal is only performed after:

- authorisation by the Security Officer or Systems & Infrastructure Manager, and
- removal of volatile and non-volatile memory components.

Hardware Security Modules and computer equipment that contains or has contained private key material (excluding operator smart cards) is only removed from Digi-Sign for servicing or disposal following authorisation from the Security Officer or Systems & Infrastructure Manager.

Information assets and equipment containing storage media, e.g. fixed hard disks, must be checked to ensure that action is taken to deface or remove sensitive data and licensed software prior to decommissioning and disposal of the assets or equipment.

5.1.8. Off-Site Backup

A secure site must be used for the storage and retention of off-site backup software and data. The off-site storage must have an equivalent level of physical security access control as the Digi-Sign offices and operations centre.

5.2. Procedural Controls

5.2.1. Trusted roles

Digi-Sign contains a number of designated ‘ positions of trust’ . These positions underpin the secure and reliable operation of the PKI, and as such must be filled by competent and trustworthy people (although several positions of trust may be filled by the same person). The general principle is that any role providing an opportunity to compromise private key material or impact on the certificate life cycle must be a trusted role.

5.2.2. Number of persons required per task

Multi-person control is used where feasible to provide enhanced security and checks and balances over PKI operations. 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. In particular:

- the Security Officer always remains separate from the System Operators in order to provide an independent review of the audit log
- CA private keys are under dual control using split passphrases and/or tamper evident HSMs.

5.2.3. Identification and authentication for each role

Digi-Sign employees in trusted roles have their identity confirmed as part of the "fit and proper person" check required under the *Code of Practice for Recognized Certification Authorities.*

Staff members are given separate accounts with access and privileges granted according to "need-to-use" and "event-by-event" principles. Use of group accounts is restricted to access of public information and for temporary, limited time use only.

5.3. Personnel Security Controls

5.3.1. Background, qualifications, experience and clearance requirements

All Digi-Sign personnel must have the requisite qualifications, experience and clearance requirements to perform their duties, and be a "fit and proper person" as defined in the *Code of Practice for Recognized Certification Authorities*.

5.3.2. Background check procedures

The Digi-Sign personnel clearance process includes formal vetting procedures including a comprehensive background check.

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)*.

5.3.3. Training requirements

The Digi-Sign Security Officer is responsible for education and training, which includes the following:

- The Digi-Sign *Security Policy* and *Information Security Guidelines and Practices*
- specific security practices and business controls for the applicable system(s)
- security awareness as part of staff induction and also on-going.

5.3.4. Retraining frequency and requirements

The introduction of any new security procedure or major software release must be accompanied by a corresponding education program for affected staff, to ensure that they are aware of their new responsibilities. Remedial training is completed when recommended by audit comments.

5.3.5. Job rotation frequency and sequence

Digi-Sign will implement either formal job rotation practices or cross-training in order to ensure operations continuity.

5.3.6. Sanctions for unauthorised actions

Where a staff member has been found to have seriously misused the resources to which they have been granted access, these actions shall be documented and passed to Digi-Sign' s Chief Executive Officer, who may wish to take disciplinary action.

Sanctions against contract employees shall be in accordance with the terms and conditions of their contract.

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 Code of Ethics and Conduct further sets the direction for disciplinary action and termination procedures respectively. Depending on the nature of the actions sanctions may range from counselling and/or suspension of access rights, through to dismissal and/or legal action.

5.3.7. Contracting personnel requirements

Where contractors are employed within Digi-Sign, their rights and obligations and all terms and conditions of service will be as per the applicable contract. Casual staff and third party users who are not already covered by an existing contract (containing a confidentiality agreement) may be required to sign a Confidentiality Agreement or other undertaking before being granted limited access to information processing facilities.

5.3.8. Documentation supplied to personnel

All Digi-Sign operational personnel have access to the following documentation:

- all relevant hardware and software documentation
- application manuals where appropriate
- policy documents, including this CPS
- operational practice and procedure documents, including the CPS and the Digi-Sign *Information Security Guidelines and Practices* as appropriate.

Note that the Digi-Sign PKI is largely composed of commercial-off-the-shelf products. Software documentation is therefore widely available to staff.

General documents relating to the operation of the PKI such as this CPS and the privacy policy will be made freely available to Digi-Sign employees, for example through publication on the Digi-Sign website. Access to more sensitive documents such as detailed security or operational documents is limited to appropriately vetted personnel and only provided on a need-to-know basis.

6. TECHNICAL SECURITY CONTROLS

Section 6: Technical Security Controls: This section defines the security measures taken by the issuing CA to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares). Section 6 imposes constraints on Digi-Sign and Subscribers to protect their cryptographic keys and critical security parameters. Secure key management is critical to ensure that all secret and private keys and activation data are protected and used only by authorized personnel. Section 3 also describes other technical security controls used to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, audit, and archival. Technical controls include life-cycle security controls (including software development environment security, trusted software development methodology) and operational security controls.

6.1. Key Pair Generation and Installation

6.1.1. Key pair generation

Key pairs for CAs, RAs and Subscribers must be generated in a manner that ensures the private key is known only to the authorised user of the key pair. All keys must be generated in accordance with the relevant CP. The CP includes details of the key algorithm, key length, validity period, and usage constraints.

Generally, Digi-Sign CA keys are generated on the device that uses them. The "General Purpose" CA keys are generated on the relevant Hardware Security Module (HSM). The Digi-Sign Root CA keys and CA keys are generated and installed by Digi-Sign in accordance with the *Digi-Sign CA Key Management Procedures*, requiring the presence of two authorizers to supervise the generation, installation, and access processes, using a FIPS 140-1 level 4 certified HSM.

Subscriber private keys may be generated by the relevant Subscriber, or by Digi-Sign. In the latter instance, the keys are generated within the Digi-Sign premises, using the Digi-Sign trustworthy system. This utilises segregation of duties to generate the keys, copy the key and certificate to the applicable storage medium, generate the PIN and print the PIN Mailer. Subscriber self key generation is only permitted in strictly controlled circumstances, as set out in the applicable CP.

6.1.2. Private Key delivery to entity

In cases of Subscriber generated keys there is no requirement for private key delivery to entity.

In cases of centrally generated keys, following secure generation, the private key is delivered to the Subscriber according to the procedures set out in the applicable CP.

6.1.3. Public Key delivery to certificate issuer

In cases of central key generation by Digi-Sign, there is no need for public key delivery as Digi-Sign has generated both the public and private keys.

In cases of Subscribers generating their own keys, the Subscriber' s public key must be transferred to the issuing Digi-Sign CA in a way that ensures that:

- it has not been changed during transit
- the sender possesses the private key that corresponds to the transferred public key, and
- the sender of the public key is the legitimate user claimed in the certificate application.

6.1.4. CA Public Key delivery to users

The public keys of each Digi-Sign CA key pair are published on the Digi-Sign website: <www.dg-sign.com>.

6.1.5. Key sizes

The Digi-Sign CAs have keys with a length of 2048 bits.

Subscriber keys are usually 1024 bits. (Consult applicable CP for confirmation).

6.1.6. Public Key parameters generation

Not applicable. All keys used within the Digi-Sign "General Purpose" PKI, including Subscriber keys, are generated using the RSA algorithm. The RSA algorithm does not require the generation of parameters.

6.1.7. Parameter quality checking

Not applicable. All keys used within the Digi-Sign "General Purpose" PKI, including Subscriber keys, are generated using the RSA algorithm. The RSA algorithm does not require the generation of parameters.

6.1.8. Hardware/software key generation

The Digi-Sign "General Purpose" PKI uses a mixture of hardware crypto-modules and software in order to generate the various CA, RA and Subscriber keys used throughout the system.

6.1.9. Key usage purposes

Keys may only be used for the purposes and in the manner described in the applicable CP. The restrictions described in the CP must be observed.

In some cases, Subscribers require two separate certificates and key pairs – one used for confidentiality (encryption) and the other used for authentication (signing) purposes. (This is so the private confidentiality key may be escrowed if desired by the private confidentiality key owner in order to retrieve data encrypted under a lost key).

Other situations only require one key pair and certificate per Subscriber.

This will usually be specified in the applicable CP.

6.2. Private Key Protection

6.2.1. Standards for cryptographic module

Digi-Sign CA key generation, storage and signing operations must be performed using a hardware-based cryptographic module rated at FIPS 140-1 Level 4.

If Subscribers generate their own private keys, the private key generation must also be done using a hardware-based cryptographic module rated at FIPS 140-1 Level 3 (or higher).

6.2.2. Private key (n out of m) multi-person control

Subscriber private keys must not be made subject to multi-person control. Generally, there is a one to one relationship between Subscribers and private keys, and Subscribers should not share their private key or disclose their private key to others.

In some circumstances there may be a role-based private key shared by several authorized users who perform a common role. If private keys are to be shared in this manner, it must be explicitly stated in the applicable CP.

All use, backup and archival of any Digi-Sign CA private key is subject to multi-person control, requiring the presence of two authorizers.

6.2.3. Private key escrow

Currently, no Subscriber key escrow service is provided.

6.2.4. Private key backup

Backups are maintained of Digi-Sign CA and RA private keys. These backup private keys are created immediately following key generation, and stored and maintained subject to an equivalent level of security to the live keys.

Subscriber private key backup is the responsibility of the individual Certificate Holder.

6.2.5. Private key archival

Upon expiry or revocation of any of the Digi-Sign CA keys and certificates, Digi-Sign archives the relevant private key in a suitable storage device and securely retains it in archive for seven years.

The issuing CA does not escrow or otherwise archive Subscriber private keys.

6.2.6. Private key entry into cryptographic module

In general, if a cryptographic module is used, the CA private key must be generated in it and remain there in both encrypted and decrypted forms, and be decrypted only at the time at which it is being used.

For details regarding Subscriber private keys refer to the applicable CP.

6.2.7. Method of activating private key

Subscriber keys are activated using memorised activation data, i.e. the Subscriber' s passphrase. Activation of a Subscriber private key by anyone other than the authorized Subscriber is forbidden (subject to any exceptions listed in the applicable CP).

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.

It is possible that Digi-Sign will deploy biometric key activation for both the CA and Subscribers in the future.

6.2.8. Method of deactivating private key

Upon termination of the CA application using the private key, the system will automatically deactivate the CA private key.

The usual means of deactivation for Subscriber keys is for the Subscriber to log off the relevant application.

6.2.9. Method of destroying private key

All CA private authentication keys must be rendered unusable once no longer needed by the authorized key custodian so that no unauthorized use can occur. The key custodian must record the destruction of the key.

In extraordinary circumstances, it may be necessary to destroy a private key to ensure integrity and protection of Digi-Sign PKI operations. Emergency disposal must be authorised by the Security Officer and a member of the PAA.

Control of the CA keys is set out in the document *CA Key Management Procedure*, including initialization of the CA key tokens and revocation of the CA public keys.

Disposal of Subscriber private keys, once expired, is the responsibility of the Subscriber.

6.3. Other Aspects of Key Pair Management

6.3.1. Public key archival

All public keys, including Subscriber public keys in cases of centralized generation, are archived by the certifying Digi-Sign CA.

6.3.2. Usage periods for the public and private keys

Key Pair(s)	Usage Period
Subscriber confidentiality keys	Refer to applicable CP

Subscriber authentication keys	Refer to applicable CP
RA confidentiality keys	Refer to applicable CP
RA authentication keys	Refer to applicable CP
CA confidentiality keys	10 years
CA authentication keys	10 years

6.4. Activation Data

Activation data are data that are used and needed to activate a private key, such as a PIN or password.

6.4.1. Activation data generation and installation

All activation data is generated in a secure manner and installed and utilized in a manner that prevents disclosure to unauthorized parties. Upon generation of the Digi-Sign CA private key, the system also generates activation data to protect the CA private keys. Access to such activation data requires the login by two authorized users.

Subscriber activation data generation and installation is described in the applicable CP.

6.4.2. Activation data protection

Different forms of protection apply to different forms of activation data. Subscribers must protect their passphrases by memorizing them instead of writing them down and never disclosing them to other individuals. Subscribers are obliged to accord the same level of care and protection to activation data as to the private keys themselves.

6.5. Computer Security Controls

6.5.1. Specific computer security technical requirements

Appropriate levels of trustworthiness and security exist throughout the Digi-Sign "General Purpose" PKI. Security is equivalent to the standards mandated under the *Code of Practice for Recognized Certification Authorities.*

Specific computer system security controls in place include:

- a configuration baseline and a configuration change control process
- performance of regular and frequent systems operability tests to prove the correct operation of critical components
- strong authentication required for system access
- proactive user account management including comprehensive auditing and timely removal of access
- role segregation and dual control procedures

- restrictions and controls on the use of system utilities
- logging of all system access and use.

6.5.2. Computer security rating

Typically, products in use within Digi-Sign have security ratings when required under the *Code of Practice for Recognized Certification Authorities* or according to industry best practice.

6.6. Life Cycle Technical 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.

6.6.1. System development controls

The software development controls applied in the development of the CA and RA software have been evaluated and certified to meet the requirements of ITSEC E3.

6.6.2. Security management controls

Security management controls exist to ensure that Digi-Sign systems are operating correctly and in a manner consistent with a configuration baseline. Change control procedures exist for recording all changes to the system configuration, including all hardware and software changes.

6.6.3. Life cycle security ratings

No specific life cycle security ratings were sought in the development of the CA and RA software.

6.7. 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. The Digi-Sign network security controls include:

- firewalls
- strong authentication
- mechanisms to prevent denial-of-service attacks
- password and other access control
- network node monitoring
- intrusion detection system.

The network security controls were developed after conducting a comprehensive threat and risk assessment.

6.8. Cryptographic Module Engineering Controls

The cryptographic modules used within the Digi-Sign "General Purpose" PKI have been subjected to generally accepted testing and evaluation criteria such as FIPS 140-1. In particular, HSMs in use by Digi-Sign:

- house all critical security functions within a tamper detection envelope
- require user authentication to the module prior to activating private keys
- are PKCS #11 compliant
- are accredited to FIPS 140-1 Level 4
- feature an integrated smart card reader, keyboard and display.

7. CERTIFICATE AND CRL PROFILES

Section 7: Certificate and CRL Profiles: This section specifies the certificate format and the CRL format. This includes information on profiles, versions, and extensions used. Section 7 in the CPS is a high level description, with specific detail on particular certificate types contained in Section 7 of the CP for that certificate type.

7.1. Certificate Profile

This section describes the general content and format of Digi-Sign certificates for Subscribers. More detailed information regarding each certificate type is contained in the applicable CP.

7.1.1. Version number(s)

These are X.509 version 3 certificates. This is indicated by the presence of a "V3" in the version field.

7.1.2. Certificate extensions

The following X.509 version 3 extensions are generally used in Digi-Sign "General Purpose" certificates:

- Key usage
- Authority key identifier
- Subject key identifier
- CRL signature
- Certificate policies.

7.1.3. Algorithm object identifiers

The Digi-Sign CA certificates use the RSA encryption algorithm and the SHA-1 hash function. The Subscriber certificates use RSA encryption and may use various hash algorithms, for example SHA-1 or MD-5. Refer to the applicable CP.

7.1.4. Name forms

ELEMENT	X.521 ATTRIBUTE TYPE	VALUE	
		Issuer	Subject
Country	countryName	HK	HK

ELEMENT	X.521 ATTRIBUTE TYPE	VALUE	
		Issuer	Subject
Organisation	organizationName	DIGI-SIGN CERTIFICATION SERVICES LIMITED	*Refer to CP*
Organisational Unit	organizationalUnitName	BRN 31346952-000	*Refer to CP*
Common Name	commonName	ID-CERT GENERAL SIGNING CA CERT	*Refer to CP*

7.1.5. Name constraints

This extension is generally not used.

7.1.6. Certificate policy object identifier

This field may contain the CP' s OID. See also section 1.2 above.

7.1.7. Usage of policy constraints extension

The policy constraints extension is generally not used.

7.1.8. Policy qualifiers syntax and semantics

FIELD (SYNTAX)	Used/Not Used
CP OID	Used / Non-critical
Qualifier (CPS URI)	Used / Non-critical
Qualifier (User Notice – Explicit Text)	Used / Non-critical

7.1.9. Processing semantics for the critical certificate policy extension

The policy qualifier extension is used but is defined as non-critical. However, certificate holders and relying parties must abide by the terms and conditions of the applicable CP.

7.2. CRL Profile

This profile applies to CRLs issued by CAs within the Digi-Sign "General Purpose" PKI.

7.2.1. Version number(s)

The Digi-Sign "General Purpose" PKI supports the use of X.509 version 2 CRLs, indicated by the presence of "V2" in the version field.

7.2.2. CRL and CRL entry extensions

The Digi-Sign "General Purpose" PKI supports the use of X.509 Version 2 CRL entry extensions. For further detail, consult the applicable CP.

8. SPECIFICATION ADMINISTRATION

Section 8: Specification Administration: This section specifies how this particular CPS is maintained.

8.1. Specification Change Procedures

Changes that do not materially affect users of Digi-Sign "General Purpose" certificates may be made at the discretion of the Digi-Sign Chief Executive Officer and:

- do not require notice to be given to any subordinate CA or RA, Subscriber or relying party
- do require updating of the version number and date of publication.

Changes that do not materially affect users include editorial corrections, typographical corrections, changes to contact details and any other change deemed by the Digi-Sign Chief Executive Officer to have no effect on the level of assurance or acceptability of related certificates.

Changes that do materially affect users of Digi-Sign "General Purpose" certificates may only be made at the discretion of the Digi-Sign PAA and:

- do require notice to be given to any subordinate CA or RA, Subscriber or relying party
- do require updating of the version number and date of publication.

Changes that materially affect users include any change deemed to affect the level of assurance or acceptability of related certificates.

Material changes require the consent of the Digi-Sign PAA.

8.2. Publication and Notification Policies

End users are not notified individually about changes to this CPS. Notification follows a "pull" model, requiring interested parties to monitor the document when they feel the need to do so, and retrieve amendments when they occur. This approach is appropriate as the Digi-Sign "General Purpose" certificates issued under this CPS are usually intended for use within a "closed" PKI.

(Digi-Sign recommends use of Recognized certificates for transactions with third parties).

8.3. CPS Approval Procedures

The Digi-Sign PAA determines whether or not this CPS provides suitable support for associated CPs.

A. ANNEX A: CERTIFICATE POLICIES THIS CPS SUPPORTS

This CPS supports the following CPs:

Certificate Policy	Short Title	Object Identifier (OID)	Comments
Undisclosed	Undisclosed	1.3.6.1.4.1.8420.5.1.0	Undisclosed
Undisclosed	Undisclosed	1.3.6.1.4.1.8420.7.1.0	Undisclosed
BOCHK Certificate Policy	BOCHK CP	1.3.6.1.4.1.8420.15.1.0	N/A