Digi-Sign (Digi-Sign Certification Services Limited) - China CITIC Bank International Limited

# Certificate Policy

**November 2012**

**(OID: 1.3.6.1.4.1.8420.5.1.2)**

Table of Contents

**1. INTRODUCTION .......... 7**

1.1. OVERVIEW .......... 7

1.2. POLICY IDENTIFICATION .......... 7

1.2.1. Certificate Policy (CP) Identification .......... 7

1.2.2. CPS Identification .......... 7

1.3. COMMUNITY AND APPLICABILITY .......... 7

1.3.1. Policy Approval Authority .......... 8

1.3.2. Certification Authority (CA) .......... 8

1.3.3. Registration Authority .......... 8

1.3.4. Subscribers .......... 8

1.3.5. Relying Parties .......... 8

1.3.6. Applicability .......... 8

1.4. CONTACT DETAILS .......... 9

1.4.1. Person determining CPS suitability for this policy .......... 9

1.5. RELATIONSHIP BETWEEN THIS CP AND THE ASSOCIATED CERTIFICATION PRACTICE STATEMENT (CPS) 9

1.5.1. Hierarchy of documents .......... 9

**2. GENERAL PROVISIONS .......... 10**

2.1 OBLIGATIONS .......... 10

2.1.1. Root Certification Authority (RCA) Obligations .......... 10

2.1.2. Certification Authority (CA) Obligations .......... 10

2.1.3. Registration Authority Officer Obligations .......... 10

2.1.4. Subscriber Obligations .......... 11

2.1.5. Repository Obligations .......... 11

2.1.6. Relying Parties Obligations .......... 12

2.2. LIABILITY .......... 12

2.3. FINANCIAL RESPONSIBILITY .......... 12

2.3.1. Indemnification of CA .......... 12

2.3.2. Fiduciary Relationships .......... 13

2.3.3. Administrative Processes .......... 13

2.4. INTERPRETATION AND ENFORCEMENT .......... 13

2.4.1. Governing Law .......... 13

2.4.2. Dispute Resolution .......... 13

2.5. FEES .......... 13

2.6. PUBLICATION AND REPOSITORIES .......... 14

2.6.1. Publication of CA information .......... 14

2.6.2. Frequency of Publication ........ 14
2.6.3. Access Control ........ 14
2.7. COMPLIANCE AUDIT ........ 14
2.8. CONFIDENTIALITY ........ 14
2.9. INTELLECTUAL PROPERTY RIGHTS ........ 14
2.9.1. Attribution ........ 14

**3. IDENTIFICATION AND AUTHENTICATION ........ 16**

3.1. INITIAL REGISTRATION ........ 16
3.1.1. Types of names ........ 16
3.1.2. Need for names to be meaningful ........ 16
3.1.3. Rules for interpreting various name forms ........ 16
3.1.4. Uniqueness of names ........ 16
3.1.5. Name claim dispute resolution procedure ........ 16
3.1.6. Recognition, authentication and role of trademarks ........ 17
3.1.7. Method to prove possession of private key ........ 17
3.1.8. Authentication of organization identity ........ 17
3.1.9. Authentication of individual identity ........ 17
3.2. CERTIFICATE RENEWAL ........ 17
3.3. RENEWAL AFTER REVOCATION ........ 18
3.4. REVOCATION REQUEST ........ 18

**4. OPERATIONAL REQUIREMENTS ........ 19**

4.1. CERTIFICATE APPLICATION ........ 19
4.2. CERTIFICATE ISSUANCE ........ 19
4.3. CERTIFICATE ACCEPTANCE ........ 19
4.4. CERTIFICATE SUSPENSION AND REVOCATION ........ 20
4.4.1. Circumstances for revocation ........ 20
4.4.2. Who can request revocation ........ 20
4.4.3. Procedure for revocation request ........ 20
4.4.4. Revocation request grace period ........ 22
4.4.5. Circumstances for suspension ........ 22
4.4.6. Who can request suspension ........ 22
4.4.7. Procedure for suspension request ........ 22
4.4.8. Limits on suspension period ........ 23
4.4.9. CRL issuance frequency ........ 23
4.4.10. CRL checking requirements ........ 23
4.4.11. On-line revocation/status checking availability ........ 23
4.4.12. On-line revocation checking requirements ........ 23

4.4.13. Other forms of revocation advertisments available ....23
4.4.14. Checking requirements for other forms of revocation advertisments ....23
4.4.15. Special requirements re key compromise ....23
4.5. SECURITY AUDIT PROCEDURES ....23
4.6. RECORDS ARCHIVAL ....23
4.6.1. Types of event recorded ....23
4.6.2. Retention period for archive ....23
4.6.3. Protection of archive ....24
4.6.4. Archive backup procedures ....24
4.6.5. Requirements for time-stamping of records ....24
4.6.6. Archive collection system (internal or external) ....24
4.6.7. Procedures to obtain and verify archive information ....24
4.7. KEY CHANGEOVER ....24
4.7.1. Key changeover and archiving ....24
4.8. COMPROMISE AND DISASTER RECOVERY ....24
4.8.1. Computing resources, software and/or data are corrupted ....24
4.8.2. Entity public key is revoked ....24
4.8.3. Entity key is compromised ....24
4.8.4. Secure facility after a natural or other type of disaster ....24
4.9. CA TERMINATION ....24

**5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS ....26**

5.1. PHYSICAL SECURITY CONTROLS ....26
5.1.1. Site Location and Construction ....26
5.1.2. Physical Access ....26
5.1.3. Power and Air Conditioning ....26
5.1.4. Water Exposures ....26
5.1.5. Fire Prevention and Protection ....26
5.1.6. Media Storage ....26
5.1.7. Waste Disposal ....26
5.1.8. Off-Site Backup ....26
5.2. PROCEDURAL CONTROLS ....27
5.2.1. Trusted roles ....27
5.2.2. Number of persons required per task ....27
5.2.3. Identification and authentication for each role ....27
5.3. PERSONNEL SECURITY CONTROLS ....27
5.3.1. Background, qualifications, experience and clearance requirements ....27
5.3.2. Background check procedures ....27
5.3.3. Training requirements ....27

5.3.4. Retraining frequency and requirements ....27
5.3.5. Job rotation frequency and sequence ....27
5.3.6. Sanctions for unauthorised actions ....27
5.3.7. Contracting personnel requirements ....27
5.3.8. Documentation supplied to personnel ....27

**6. TECHNICAL SECURITY CONTROLS ....28**

6.1. KEY PAIR GENERATION AND INSTALLATION ....28
6.1.1. Key pair generation ....28
6.1.2. Private Key delivery to entity ....28
6.1.3. Public Key delivery to certificate issuer ....28
6.1.4. CA Public Key delivery to users ....28
6.1.5. Key sizes ....28
6.1.6. Public Key parameters generation ....29
6.1.7. Parameter quality checking ....29
6.1.8. Hardware/software key generation ....29
6.1.9. Key usage purposes ....29
6.2. PRIVATE KEY PROTECTION ....29
6.2.1. Standards for cryptographic module ....29
6.2.2. Private key (n out of m) multi-person control ....29
6.2.3. Private key escrow ....29
6.2.4. Private key backup ....29
6.2.5. Private key archival ....29
6.2.6. Private key entry into cryptographic module ....29
6.2.7. Method of activating private key ....29
6.2.8. Method of deactivating private key ....30
6.2.9. Method of destroying private key ....30
6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT ....30
6.3.1. Public key archival ....30
6.3.2. Usage periods for the public and private keys ....30
6.4. ACTIVATION DATA ....30
6.4.1. Activation data generation and installation ....30
6.4.2. Activation data protection ....30
6.5. COMPUTER SECURITY CONTROLS ....31
6.5.1. Specific computer security technical requirements ....31
6.5.2. Computer security rating ....31
6.6. LIFE CYCLE TECHNICAL CONTROLS ....31
6.6.1. System development controls ....31
6.6.2. Security management controls ....31

6.6.3. Life cycle security ratings .....31
6.7. NETWORK SECURITY CONTROLS .....31
6.8. CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS .....31

**7. CERTIFICATE AND CRL PROFILES .....32**

7.1.1. Version number(s).....32
7.1.2. Certificate extensions .....32
7.1.3. Algorithm object identifiers .....32
7.1.4. Name forms.....33
7.1.5. Name constraints.....33
7.1.6. Certificate policy object identifier.....33
7.1.7. Usage of policy constraints extension .....33
7.1.8. Policy qualifiers syntax and semantics.....33
7.1.9. Processing semantics for the critical certificate policy extension .....34
7.2. CRL PROFILE.....34

**8. SPECIFICATION ADMINISTRATION .....35**

8.1. SPECIFICATION CHANGE PROCEDURES.....35
8.2. PUBLICATION AND NOTIFICATION POLICIES .....35
8.2.1. CP Publication and Notification.....35
8.3. CPS / CP APPROVAL PROCEDURES.....35

# 1. INTRODUCTION

*Section 1: Introduction*: This section identifies and introduces the Certificate Policy (CP) provisions, and indicates the types of entities and applications for which the CP is targeted.

## 1.1. Overview

This Certificate Policy (CP) is the Digi-Sign Certification Services Ltd ("Digi-Sign") and China CITIC Bank International Ltd ("CNCBI") CP. It describes the practices and procedures involved in the issuance of public key digital certificates by Digi-Sign's "General Purpose" PKI hierarchy for the CNCBI's customers.

## 1.2. Policy Identification

### 1.2.1. Certificate Policy (CP) Identification

This CP has been allocated the OID: 1.3.6.1.4.1.8420.5.1.2, constructed as follows:

| | |
|---|---|
| 1.3 | ISO assigned / ISO identified organization |
| 6.1.4.1 | Internet related IANA registered private enterprise |
| 8420 | Digi-Sign Certification Services Limited |
| 5 | CNCBI CP document number |
| 1.0 (example) | Version number |

### 1.2.2. CPS Identification

The accompanying CPS to this CP has been allocated the OID: 1.3.6.1.4.1.8420.4.N.N, where N.N indicates the version number. 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 CP is applicable to:

- the Digi-Sign "General Purpose" Certification Authority
- the CNCBI's Registration Authority Operator (RAO)
- subscribers, being the CNCBI's Registered Users.

### 1.3.1. Policy Approval Authority

The practices and procedures in this CP 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) within its certificate policy domains. Under this CP, the Digi-Sign CA will issue “General Purpose” certificates to Registered Users of CNCBI.

### 1.3.3. Registration Authority

The Registration Authority (RA) is subordinated to the CA. The primary purpose of the RA is to receive and authenticate subscribers' applications for the issuance of certificates and revocation requests. Under this CP, the registration function, including obtaining evidence of identity, registering subscribers and records retention are to be performed by CNCBI.

### 1.3.4. Subscribers

Subscribers under this CP are the CNCBI Registered Users (i.e. organizations who are customers of CNCBI and apply to Digi-Sign through CNCBI for issuance of keys and certificates).

### 1.3.5. Relying Parties

The only parties authorized to rely on these certificates are CNCBI and CNCBI’s corporate internet banking customers.

### 1.3.6. Applicability

#### 1.3.6.1. General Purpose

These certificates are to be used for CNCBI’s corporate internet banking services.

#### 1.3.6.2. Restrictions on Use

These certificates may only be used for the purposes and in the manner described within this CP.

#### 1.3.6.3. Prohibitions on Use

These certificates are not to be used for applications which have not been authorized by CNCBI.

## 1.4. Contact Details

Refer to the CPS.

### 1.4.1. Person determining CPS suitability for this policy

The Digi-Sign PAA will determine whether the accompanying CPS provides suitable support for this CP. The PAA will review both documents to ensure that the practices documented in the CPS fulfil the requirements defined in this CP.

## 1.5. Relationship between this CP and the associated Certification Practice Statement (CPS)

This CP defines and limits the use of certificates issued to CNCBI's Registered Users. This CP is supported by the Digi-Sign "General Purpose" CPS, which explains how the requirements of the CP are met in procedural and operational terms.

### 1.5.1. Hierarchy of documents

The 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 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, this CP will take precedence over the CPS.

The *Digi-Sign General Purpose Certificate Service Agreement* between Digi-Sign and CNCBI takes 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. These provisions must be considered in conjunction with the broad principles set out in the CPS and the terms and provisions of the *Digi-Sign General Purpose Certificate Service Agreement*. In case of conflict, the *Digi-Sign General Purpose Certificate Service Agreement* overrides the CP and CPS.

## 2.1 Obligations

### 2.1.1. Root Certification Authority (RCA) Obligations

Refer to CPS.

### 2.1.2. Certification Authority (CA) Obligations

Refer to CPS.

### 2.1.3. Registration Authority Officer Obligations

CNCBI shall perform the Registration Authority Officer (RAO) function for the Digi-Sign CA under this CP. As RAO, CNCBI accepts the following obligations:

- Accepting certificate applications including obtaining evidence of organization identity, obtaining certificate applications information and accepting or rejecting applications
- Advising Registered Users (subscribers) of their obligations, including their duty to safeguard their private keys and promptly report any compromise or suspected compromise
- Submitting certificate requests that are factually correct from the information known to the RAO at time of submission, and that are free from data entry errors
- Keeping such registration records during the validity of the relevant certificate
- Ensure that Registered Users execute the relevant documents in the form approved by Digi-Sign and CNCBI, which approval shall not be unreasonably withheld or delayed by either Digi-Sign or CNCBI.
- Comply with all notices, instructions and manuals issued by Digi-Sign from time to time
- Comply with this CP, the associated CPS and the Digi-Sign General Purpose Certificate Service Agreement
- Indemnify Digi-Sign against any actual direct costs reasonably incurred by Digi-Sign to the extend attributable to a failure to observe these obligations and the requirements of the CPS and the Digi-Sign General Purpose Certificate Service Agreement.

For the avoidance of doubt, neither CNCBI nor Digi-Sign shall be responsible for authentication of the identity of any message signatories of any subscribers, in relation to or in connection with their certificate applications.

### 2.1.4. Subscriber Obligations

Subscribers under this CP are the Registered Users of CNCBI Subscriber obligations include:

- Understand and comply with all directions from CNCBI when using the certificate and the private key;
- Use the certificate and the private key strictly in accordance with this CP, any applicable written contract and the CPS;
- Provide true and correct information upon applying for key and certificate and notify the RAO immediately of any changes thereafter;
- Notify the RAO 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 certificate has been used in any transaction or communication between the subscriber and the relying party;
- Undertake to stop the use of the certificate immediately upon the following:
    - The subscriber has lodged a request with the RAO to revoke the certificate, or has been notified by the RAO of the revocation of the certificate; or
    - The subscriber has become aware of any event that Digi-Sign would normally rely upon as reason for revocation of the certificate, as listed in section 4.4.1 of this CP or the CPS.
- Undertake not to:
    - Use the private key in a manner that may infringe the rights of a third party; or
    - Assign any rights under the Subscriber Agreement or other applicable contract.
- Indemnify Digi-Sign against any actual direct costs reasonably incurred by Digi-Sign to the extend attributable to the subscriber's:
    - failure to maintain the protection of the private key; or
    - misuse of the private key.

### 2.1.5. Repository Obligations

Refer to CPS.

### 2.1.6. Relying Parties Obligations

For the purpose of this CP, the act of acceptance of a certificate issued under this CP is referred to as reliance on the certificate and the digital signature of the subscriber. The relying party has a duty to decide whether to rely on the certificate. Once this relying party has decided to do so, it has the obligation to:

- Understand the usage for which the certificate is issued; and
- Accept the responsibility to:
  - Check if the certificate or the issuing CA's certificate have been suspended or revoked before relying on it; and
  - Check if the certificate or the issuing CA's certificate have expired before relying on it; and
  - Verify the digital signature, including the performance of all appropriate certificate path validation procedures.
- Accept that the use of the certificate is subject to applicable liability and warranty disclaimers outlined in section 2.2 *Liability* of this CP.
- Accept that the use of the certificate is specifically for the limited purpose as outlined in Section 1.3 *Community and Applicability* of this CP, particularly as to any restrictions and prohibitions on use.

## 2.2. Liability

The warranties expressly specified in:

- the *Digi-Sign General Purpose Certificate Service Agreement* between Digi-Sign and CNCBI, and
- the Digi-Sign "General Purpose" CPS associated with this CP

are the sole and exclusive warranties given by Digi-Sign. No implied or other 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.

Digi-Sign's liability, if any, is limited according to the terms and provisions contained in the *Digi-Sign General Purpose Certificate Service Agreement* between Digi-Sign and CNCBI. However, Digi-Sign shall in any event not be liable to the subscribers or any relying parties for loss or damages in excess of a liability cap of HK$200,000.00 ("the Liability Cap") in respect of one certificate and irrespective of the number of transactions involved in that one certificate and irrespective of whether the loss or damages are caused by the negligence or default of Digi-Sign.

## 2.3. Financial Responsibility

### 2.3.1. Indemnification of CA

CNCBI and Digi-Sign shall indemnify and at all time keep each other fully indemnified for all loss and damage suffered to the extend solely and directly resulting from:

- all breach, non compliance or non observance of the terms and conditions in this CP, the CPS or the Digi-Sign General Purpose Certificate Service Agreement by the other party; or
- any fraud or deception committed by or other act of dishonesty of the other party.

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 CP, the CPS or the Digi-Sign General Purpose Certificate Subscriber Agreement; or
- any fraud or deception committed by or other act of dishonesty of the subscriber.

### 2.3.2. Fiduciary Relationships

Issuing certificates under this CP, or assisting in the issue of these certificates, does not make Digi-Sign an agent, fiduciary, trustee, or other representative of CNCBI, any CNCBI's Registered User, any relying party or other third party.

### 2.3.3. Administrative Processes

No stipulation.

## 2.4. Interpretation and Enforcement

### 2.4.1. Governing Law

This CP and the associated CPS and Digi-Sign General Purpose Certificate Service Agreement are governed by and construed in accordance with the laws of Hong Kong and the parties unconditionally and irrevocably submit to the non-exclusive jurisdiction of the courts of Hong Kong SAR.

### 2.4.2. Dispute Resolution

If a dispute arises the parties to the dispute will endeavor in good faith to settle the dispute by negotiation. The parties may also elect, if they so desire, to settle dispute using mediation and/or arbitration. Parties reserve the right to resolve disputes through litigation in the courts of Hong Kong SAR.

## 2.5. Fees

CNCBI shall pay to Digi-Sign the sums as specified in the *Digi-Sign General Purpose Certificate Service Agreement* between Digi-Sign and CNCBI for the establishment of the service and for each key pair generated by Digi-Sign under this CP, along with any other fees as may be listed in that Agreement.

## 2.6. Publication and Repositories

Refer to CPS.

### 2.6.1. Publication of CA information

Refer to CPS.

#### 2.6.1.1. Publication of Policy and Practice Information

Refer to CPS.

### 2.6.2. Frequency of Publication

#### 2.6.2.1. Frequency of Certificate Publication

CNCBI certificates will not be published to the Digi-Sign's repository.

#### 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 use its best endeavors to publish an updated CRL at least once every 24 hours.

### 2.6.3. Access Control

Refer to CPS.

## 2.7. Compliance Audit

Refer to CPS.

## 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 this CP belong to and will remain the property of Digi-Sign.

### 2.9.1. Attribution

The use of these documents in the preparation of this CP 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 the CNCBI RAO prior to certificate issuance. It also describes requesting re-key and revocation. Section 3 also addresses naming practices, including name ownership recognition and name dispute resolution. Section 3 of this CP must be considered in conjunction with the relevant sections of the CPS and the *Digi-Sign General Purpose Service Agreement.*

## 3.1. Initial registration

### 3.1.1. Types of names

These certificates contain the name of the subscriber in the X.509 certificate field *SubjectName.* This field is a unique identifier of the subject and contains a standards-based Distinguished Name, constructed as follows:

CN = [Name of message signatory. Max 50 char] ([CNCBI Reference])

OU = [Subscriber Reference Number (SRN) assigned by Digi-Sign]

OU = [CNCBI Reference]

OU = [Organization Dept / Unit Name]

OU = [Organization Name]

O = CNCBI (CLASS A)

C = HK

### 3.1.2. Need for names to be meaningful

Names used within Digi-Sign “General Purpose” CNCBI certificates are intended to indicate a binding between a public key and a real-world identity and anonymous or pseudonymous certificates are not supported.

### 3.1.3. Rules for interpreting various name forms

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

### 3.1.4. Uniqueness of names

Names must be unambiguous and unique.

### 3.1.5. Name claim dispute resolution procedure

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.

### 3.1.6. Recognition, authentication and role of trademarks

Refer to CPS.

### 3.1.7. Method to prove 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 public key certificate will be stored on appropriate storage media for dispatch to CNCBI for onward dispatch to the subscriber, and this will be done in a secure manner. As all keys are centrally generated, there is no requirement for the CNCBI's Registered User to prove possession of the private key.

### 3.1.8. Authentication of organization identity

Authentication of organization identity is the responsibility of the CNCBI RAO. Digi-Sign accepts no liability resulting from errors in the authentication of an organization's identity under this CP.

### 3.1.9. Authentication of individual identity

The CNCBI RAO shall be responsible for authentication of the authorization of the message signatories of any subscribers. No authentication of individual identity of the message signatories will be conducted by Digi-Sign nor CNCBI. Such subscribers shall be solely responsible for the authentication of the identity of individual message signatories nominated by them and ensuring that the information of such message signatories provided to Digi-Sign is true and correct. Such subscribers shall in any event be bound by any transactions duly authenticated by a certificate issued pursuant hereto irrespective of the identity of the message signatories who make use of the certificate for and on behalf of such subscribers. Digi-Sign and CNCBI accept no liabilities whatsoever for any loss or damages suffered by any relying parties arising out of or in relation to discrepancies or errors in the identity of the message signatories of such subscribers.

For the avoidance of doubt, neither CNCBI nor Digi-Sign shall be responsible for the authentication of the identity of any message signatories of any subscribers.

## 3.2. Certificate Renewal

Digi-Sign does not renew a General Purpose certificate for the CNCBI's customers. Upon approval of the application submitted by CNCBI, Digi-Sign will generate a new key pair and certificate pursuant to the applicable procedure, as replacement before expiry of the subscriber's existing key pair and certificate.

Before a certificate is due to expire, Digi-Sign will issue an expiry notice to CNCBI. It will be up to CNCBI to coordinate with the subscriber to apply, and this should be done before the existing certificate expiry date.

Digi-Sign will be responsible for verifying the application against the information held in the Digi-Sign subscriber database and approving such application.

Upon approval of the application, Digi-Sign will generate a new key pair and certificate for the subscriber. Digi-Sign will follow the procedures in section 4.2 and section 4.3 as a means of confirmation of the receipt of the new key pair and certificate by the subscriber.

Notwithstanding any provisions hereof to the contrary, nothing in this CP shall constitute any agreement or promise on the part of Digi-Sign to issue, or an option available to the subscriber to demand issuance of, a new certificate to replace the one due to expire soon. Digi-Sign reserves its absolute right to refuse the subscriber's application for issuance of any certificate without giving any reasons.

## 3.3. Renewal after Revocation

Re-key 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.

## 3.4. Revocation Request

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

# 4. OPERATIONAL REQUIREMENTS

*Section 4: Operational Requirements*: This section specifies requirements imposed upon issuing CA, subject CAs, RAs, RAOs, 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 the CPS.

## 4.1. Certificate Application

Upon submitting a Key Request File, CNCBI warrants to Digi-Sign that the information provided is true and correct to the best of its knowledge, having made all reasonable enquiries with the relevant subscribers., and when request to do so, provides further proof to substantiate the details completed therein.

It is the responsibility of CNCBI to lodge the Key Request File to Digi-Sign, Digi-Sign will undertake to notify CNCBI of the results of the applications within reasonable time (and in any event not more than 3 working days) of the decision to approve or reject the application.

Digi-Sign reserves its absolute right to change the procedure to process the applications from time to time without notice.

Key Request File must be in the format agreed by CNCBI and Digi-Sign.

## 4.2. Certificate Issuance

In order to issue a certificate under this CP, the Digi-Sign CA constructs and populates the fields of an X.509 version 3 certificate, according to the requirements agreed with CNCBI. The certificate is then signed with the Digi-Sign CA's private authentication key. The certificate profile is defined within section 7 of this CP.

## 4.3. Certificate Acceptance

Acceptance is signified by the faxed-in confirmation of the CD Checklist from CNCBI to Digi-Sign, or the subscriber's receipt of a certificate and their subsequent use of their keys and certificates. By accepting a certificate, the subscriber:

- agrees to be bound by the continuing responsibilities, obligations and duties imposed on him/it by the Subscriber Agreement, the applicable CPS and this CP
- warrants that to his/its knowledge no unauthorised person has had access to the private key associated with the certificate
- asserts that the certificate information he/it has supplied during his registration interview is truthful and has been accurately and fully published within the certificate
- undertakes to inform CNCBI and/or Digi-Sign immediately if his/its information has been changed.

## 4.4. Certificate Suspension and Revocation

### 4.4.1. Circumstances for revocation

Refer to CPS.

### 4.4.2. Who can request revocation

Refer to CPS.

### 4.4.3. Procedure for revocation request

Digi-Sign will revoke a certificate if:

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

(a) Revocation as determined by Digi-Sign

Digi-Sign may decide to revoke a certificate in certain circumstances including, but not limited to, when:

(1) It is required to revoke the certificate by regulations, or by law;

(2) It is determined that the certificate

- was issued improperly, or was not issued in accordance with this CP
- 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 certificate in accordance with this CP;
- the subscriber has failed to meet the subscriber obligations set out in this CP;

(5) It is established that:

- the subscriber organisation 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 company's assets;
- a director, or public officer of the subscriber company has been convicted of an offence under the Electronic Transactions Ordinance (Cap. 553).

The decision of Digi-Sign on revocation of a certificate will be final, conclusive and binding on all parties.. Subscribers and the 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 or consequence of the revocation of a certificate by Digi-Sign (save and except loss or damage suffered directly by CNCBI out of or in connection with the negligence or default of Digi-Sign which loss or damage shall be subject to and limited by the Liability Cap of HK$200,000 in respect of one certificate and irrespective of the number of transactions involved in that one certificate).

(b) Revocation at request of CNCBI

CNCBI may at any time apply to Digi-Sign to revoke a certificate. However, CNCBI must promptly apply to Digi-Sign to revoke the certificate if it is advised by the relevant subscriber in writing 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 a certificate must be in writing and the original written request must be properly signed and delivered by CNCBI to Digi-Sign. Digi-Sign does not process requests by CNCBI to revoke a certificate via telephone.

However, CNCBI may in an emergency situation notify Digi-Sign of its intention to revoke a certificate by sending the revocation request to Digi-Sign a) by fax on a prescribed form, or b) by digitally signed email using the Key Request File (KRF). Upon receipt of such faxed-in or email notification, Digi-Sign will temporarily suspend the relevant certificate, but will not proceed to revoke the certificate. CNCBI then will send its original revocation request on the prescribed form to Digi-Sign's office within 2 working days after the faxed-in or email notification. Digi-Sign will revoke the certificate in accordance with section 4.4 upon receipt of the original revocation request. If Digi-Sign fails to receive the original revocation request within 2 working days after receiving the faxed-in or email notification, Digi-Sign will cancel the suspension and reactivate the certificate. Digi-Sign will use its best endeavours to suspend the certificate within 8 hours from the receipt of the faxed-in or email notification. If CNCBI or the subscriber need assistance, they may call the Digi-Sign hotline specified in section 1.4.1 of the CPS.

The times to receive faxed-in or email notifications are:

Monday to Friday (except public holidays): 8:30am to 6:00pm

(Excepted office closed due to tropical cyclone or black rainstorm warning signal as specified in section 1.4 of the CPS.)

Any faxed-in or email notification received outside these hours will be considered to have been received by Digi-Sign at the beginning of the next working day and processed accordingly.

Digi-Sign will provide CNCBI revocation request form in soft copy.

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 CNCBI's authorised signature in the revocation request.

Once the validity of the revocation request is established, Digi-Sign will initiate action in its trustworthy system to revoke the certificate, and update the CRL. Digi-Sign will process certificate revocation requests during the office hours as specified in section 1.4 of the CPS.

Whenever it is necessary to notify Digi-Sign of a certificate revocation request outside the above business hours, or on any day when the Digi-Sign Office is closed for business, CNCBI should call the Emergency Telephone No. in section 1.4 of the CPS herein to make arrangement.

(c) For all revocation of certificate

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

### 4.4.4. Revocation request grace period

Revocation requests are verified on receipt and are 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

Digi-Sign undertakes to issue the CRL daily.

### 4.4.10. CRL checking requirements

Refer to CPS.

### 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 re key compromise

Not applicable.

## 4.5. Security Audit Procedures

Refer to CPS.

## 4.6. Records Archival

### 4.6.1. Types of event recorded

Refer to CPS.

### 4.6.2. Retention period for archive

Refer to CPS.

### 4.6.3. Protection of archive

Refer to CPS.

### 4.6.4. Archive backup procedures

Refer to CPS.

### 4.6.5. Requirements for time-stamping of records

Refer to CPS.

### 4.6.6. Archive collection system (internal or external)

Refer to CPS.

### 4.6.7. Procedures to obtain and verify archive information

Refer to CPS.

## 4.7. Key Changeover

### 4.7.1. Key changeover and archiving

Refer to CPS.

## 4.8. Compromise and Disaster Recovery

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

Refer to CPS.

### 4.8.2. Entity public key is revoked

Refer to CPS.

### 4.8.3. Entity key is compromised

Refer to CPS.

### 4.8.4. Secure facility after a natural or other type of disaster

Refer to CPS.

## 4.9. CA Termination

Refer to CPS.

Also refer to clause 17: *Term and Termination* in the *Digi-Sign General Purpose Certificate Service Agreement.*

# 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 Digi-Sign to perform securely the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

These details are all contained in the Digi-Sign "General Purpose" CPS and are common across all Digi-Sign CA hierarchies (including recognized and general purpose) and certificate types.

## 5.1. Physical Security Controls

### 5.1.1. Site Location and Construction

Refer to CPS.

### 5.1.2. Physical Access

Refer to CPS.

### 5.1.3. Power and Air Conditioning

Refer to CPS.

### 5.1.4. Water Exposures

Refer to CPS.

### 5.1.5. Fire Prevention and Protection

Refer to CPS.

### 5.1.6. Media Storage

Refer to CPS.

### 5.1.7. Waste Disposal

Refer to CPS.

### 5.1.8. Off-Site Backup

Refer to CPS.

## 5.2. Procedural Controls

### 5.2.1. Trusted roles

Refer to CPS.

### 5.2.2. Number of persons required per task

Refer to CPS.

### 5.2.3. Identification and authentication for each role

Refer to CPS.

## 5.3. Personnel Security Controls

### 5.3.1. Background, qualifications, experience and clearance requirements

Refer to CPS.

### 5.3.2. Background check procedures

Refer to CPS.

### 5.3.3. Training requirements

Refer to CPS.

### 5.3.4. Retraining frequency and requirements

Refer to CPS.

### 5.3.5. Job rotation frequency and sequence

Refer to CPS.

### 5.3.6. Sanctions for unauthorised actions

Refer to CPS.

### 5.3.7. Contracting personnel requirements

Refer to CPS.

### 5.3.8. Documentation supplied to personnel

Refer to CPS.

# 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 CNCBI's Registered Users must be generated in a manner that ensures the private key is known only to the authorised user of the key pair. The CPS describes the use of a Hardware Security Module (HSM) for the generation of CA keys.

Keys for Registered Users are generated by Digi-Sign upon receipt of a request, in the form of a digitally signed Key Request file, from the CNCBI RAO. The keys are generated within the Digi-Sign premises, using the RSA algorithm on the Digi-Sign trustworthy system.

### 6.1.2. Private Key delivery to entity

The private keys are delivered to the Registered Users as follows:

- Digi-Sign copies the private keys generated onto secure tokens and the corresponding certificates onto a CD. It will then deliver the secure tokens and the CD to CNCBI, with a CD Checklist that displays the content of the CD. After receiving the secure tokens and the CD, CNCBI will verify the integrity of the private keys. After the verification, CNCBI then delivers the private keys to the relevant Registered User.

### 6.1.3. Public Key delivery to certificate issuer

Not applicable as keys are centrally generated by Digi-Sign.

### 6.1.4. CA Public Key delivery to users

Refer to CPS.

### 6.1.5. Key sizes

The Digi-Sign CA key length is 2048 bits. Subscriber keys are 1024 / 2048 bits.

### 6.1.6. Public Key parameters generation

Not applicable.

### 6.1.7. Parameter quality checking

Not applicable.

### 6.1.8. Hardware/software key generation

Subscriber keys issued under this CP are generated in software.

### 6.1.9. Key usage purposes

Subscriber keys issued under this CP may be used for Digital Signature, Non-Repudiation and Key Encipherment, as indicated in the key usage extension of the X.509 certificate.

## 6.2. Private Key Protection

### 6.2.1. Standards for cryptographic module

Refer to CPS.

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

Subscriber private keys must not be made subject to multi-person control.

### 6.2.3. Private key escrow

Currently, no subscriber key escrow service is provided.

### 6.2.4. Private key backup

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

### 6.2.5. Private key archival

Refer to CPS.

### 6.2.6. Private key entry into cryptographic module

Refer to CPS.

### 6.2.7. Method of activating private key

Subscriber keys are activated using memorised activation data, i.e. the subscriber's passphrase, or PIN. Activation of a subscriber private key by anyone other than the authorized subscriber is forbidden.

### 6.2.8. Method of deactivating private key

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

### 6.2.9. Method of destroying private key

Refer to CPS.

## 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 keys (utilizing a single key for authentication and confidentiality) | 3 years |
| CA confidentiality keys | 10 years |
| CA authentication keys | 10 years |

## 6.4. Activation Data

### 6.4.1. Activation data generation and installation

PINs will be generated centrally by Digi-Sign. These PINs will be encrypted and stored in the Digi-Sign database. The encrypted PINs are then decrypted, printed onto the PIN Mailer and securely distributed. After PIN Mailer delivery, the encrypted PINs stored in Digi-Sign's database will be deleted.

### 6.4.2. Activation data protection

Subscribers must protect their passphrases, or PINs 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

Refer to CPS.

### 6.5.2. Computer security rating

Refer to CPS.

## 6.6. Life Cycle Technical Controls

Refer to CPS.

### 6.6.1. System development controls

Refer to CPS.

### 6.6.2. Security management controls

Refer to CPS.

### 6.6.3. Life cycle security ratings

Refer to CPS.

## 6.7. Network Security Controls

Refer to CPS.

## 6.8. Cryptographic Module Engineering Controls

Refer to CPS.

# 7. CERTIFICATE AND CRL PROFILES

*Section 7: Certificate and CRL Profiles*: This section specifies the certificate format and the CRL format.

## 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

| **Extension** | **Used / Not Used** |
|---|---|
| Authority Key Identifier: Issuer | Not used. |
| Authority Key Identifier: Serial Number | Not used. |
| Authority Key Identifier: Public Key Identifier | Set as the Subject Key Identifier of the CA certificate used to sign this certificate. |
| Basic Constraints: Subject Type | End Entity |
| Basic Constraints: Path Length | None |
| Key Usage | Digital Signature, Non-Repudiation, Key Encipherment |
| Subject Alternative Name: DNSName | Not used. |
| Subject Alternative Name: RFC822 | E-mail address as provided by subscriber. |
| Netscape Certificate Type | SSL Client, S/MIME |
| Netscape SSL Server Name | Not used. |
| Netscape Comment | Not used. |

## 7.1.3. Algorithm object identifiers

RSA encryption algorithm, SHA-1 hash function.

Length = 1024 / 2048 bits.

### 7.1.4. Name forms

| ELEMENT | X.521 ATTRIBUTE TYPE | VALUE | |
|---|---|---|---|
| | | Issuer | Subject |
| Country | countryName | HK | HK |
| Organisation | organizationName | DIGI-SIGN CERTIFICATION SERVICES LIMITED | CNCBI (CLASS A) |
| Organisational Unit | organizationalUnitName | BRN<br>31346952-000 | 1. SRN assigned by Digi-Sign<br>2. CNCBI Reference<br>3. Organization Dept / Unit Name<br>4. Organization Name |
| Common Name | commonName | ID-CERT GENERAL SIGNING CA CERT<br>Or<br>GENERAL PURPOSE SIGNING CA CERT 1 | Name of message signatory. Maximum of 50 characters<br>And CNCBI Reference enclosed in brackets. |

### 7.1.5. Name constraints

This extension is not used.

### 7.1.6. Certificate policy object identifier

This extension is not used.

### 7.1.7. Usage of policy constraints extension

The policy constraints extension is not used.

### 7.1.8. Policy qualifiers syntax and semantics

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

### 7.1.9. Processing semantics for the critical certificate policy extension

Not applicable.

## 7.2. CRL Profile

Standard CRL profile, as per CPS.

# 8. SPECIFICATION ADMINISTRATION

*Section 8: Specification Administration*: This section specifies how this CP is maintained.

Refer to the relevant section in CPS for the CPS administration.

## 8.1. Specification Change Procedures

Changes that do not materially affect the Registered 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 the Registered 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 the Registered Users of Digi-Sign "General Purpose" certificates may be made if and only if Digi-Sign PAA and CNCBI have agreed in writing to such changes 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

### 8.2.1. CP Publication and Notification

There will not be any formal CP notification process. Rather, notification will follow a "pull" model, requiring interested parties to monitor the CP document when they feel the need to do so, and retrieve amendments when they occur.

## 8.3. CPS / CP Approval Procedures

The Digi-Sign PAA determines whether or not the Digi-Sign "General Purpose" CPS provides suitable support for associated CPs, including this CNCBI CP.