Digi-Sign Certification Services Limited

BOCHK Certificate Policy

OID: 1.3.6.1.4.1.8420.15.1.0

Based on the Digi-Sign “General Purpose” CA Hierarchy and supported by the Digi-Sign “General Purpose” CPS

Dec 2005

Table of Contents

1 INTRODUCTION.. 2

1.1. OVERVIEW 2

1.2. POLICY IDENTIFICATION 2

1.2.1. Certificate Policy (CP) Identification 2

1.2.2. CPS Identification 2

1.3. COMMUNITY AND APPLICABILITY 2

1.3.1. Policy Approval Authority.. 2

1.3.2. Certification Authority (CA).. 2

1.3.3. Registration Authority (RA) 2

1.3.4. Subscribers 2

1.3.5. Relying Parties 2

1.3.6. Applicability.. 2

1.4. CONTACT DETAILS 2

1.4.1. Person determining CPS suitability for this policy 2

1.5. RELATIONSHIP BETWEEN THIS CP AND THE ASSOCIATED CERTIFICATION PRACTICE STATEMENT (CPS) 2

1.5.1. Hierarchy of documents.. 2

2. GENERAL PROVISIONS.. 2

2.1 OBLIGATIONS.. 2

2.1.1. Root Certification Authority (RCA) Obligations.. 2

2.1.2. Certification Authority (CA) Obligations.. 2

2.1.3. Registration Authority (RA) Obligations 2

2.1.4. Subscriber Obligations.. 2

2.1.5. Repository Obligations 2

2.1.6. Relying Parties Obligations 2

2.2. LIABILITY.. 2

2.3. FINANCIAL RESPONSIBILITY 2

2.3.1. Indemnification of CA and RA.. 2

2.3.2. Fiduciary Relationships.. 2

2.3.3. Administrative Processes 2

2.4. INTERPRETATION AND ENFORCEMENT 2

2.4.1. Governing Law.. 2

2.4.2. Dispute Resolution.. 2

2.5. FEES 2

2.6. PUBLICATION AND REPOSITORIES 2

2.6.1. Publication of CA information 2

2.6.2. Frequency of Publication 2
2.6.3. Access Control 2
2.7. COMPLIANCE AUDIT 2
2.8. CONFIDENTIALITY 2
2.9. INTELLECTUAL PROPERTY RIGHTS 2
2.9.1. Attribution 2
3. IDENTIFICATION AND AUTHENTICATION 2
3.1. INITIAL REGISTRATION 2
3.1.1. Types of names 2
3.1.2. Need for names to be meaningful 2
3.1.3. Rules for interpreting various name forms 2
3.1.4. Uniqueness of names 2
3.1.5. Name claim dispute resolution procedure 2
3.1.6. Recognition, authentication and role of trademarks 2
3.1.7. Method to prove possession of private key 2
3.1.8. Authentication of organization identity 2
3.1.9. Authentication of individual identity 2
3.2. CERTIFICATE RENEWAL 2
3.3. RENEWAL AFTER REVOCATION 2
3.4. REVOCATION REQUEST 2
4. OPERATIONAL REQUIREMENTS 2
4.1. CERTIFICATE APPLICATION 2
4.2. CERTIFICATE ISSUANCE 2
4.3. CERTIFICATE ACCEPTANCE 2
4.4. CERTIFICATE SUSPENSION AND REVOCATION 2
4.4.1. Circumstances for revocation 2
4.4.2. Who can request revocation 2
4.4.3. Procedure for revocation request 2
4.4.4. Revocation request grace period 2
4.4.5. Circumstances for suspension 2
4.4.6. Who can request suspension 2
4.4.7. Procedure for suspension request 2
4.4.8. Limits on suspension period 2
4.4.9. CRL issuance frequency 2
4.4.10. CRL checking requirements 2
4.4.11. On-line revocation/status checking availability 2
4.4.12. On-line revocation checking requirements 2

4.4.13. Other forms of revocation advertisments available 2
4.4.14. Checking requirements for other forms of revocation advertisments 2
4.4.15. Special requirements re key compromise 2
4.5. SECURITY AUDIT PROCEDURES 2
4.6. RECORDS ARCHIVAL 2
4.6.1. Types of event recorded 2
4.6.2. Retention period for archive 2
4.6.3. Protection of archive 2
4.6.4. Archive backup procedures 2
4.6.5. Requirements for time-stamping of records 2
4.6.6. Archive collection system (internal or external) 2
4.6.7. Procedures to obtain and verify archive information 2
4.7. KEY CHANGEOVER 2
4.7.1. Key changeover and archiving 2
4.8. COMPROMISE AND DISASTER RECOVERY 2
4.8.1. Computing resources, software and/or data are corrupted 2
4.8.2. Entity public key is revoked 2
4.8.3. Entity key is compromised 2
4.8.4. Secure facility after a natural or other type of disaster 2
4.9. CA TERMINATION 2

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS 2

5.1. PHYSICAL SECURITY CONTROLS 2
5.1.1. Site Location and Construction 2
5.1.2. Physical Access 2
5.1.3. Power and Air Conditioning 2
5.1.4. Water Exposures 2
5.1.5. Fire Prevention and Protection 2
5.1.6. Media Storage 2
5.1.7. Waste Disposal 2
5.1.8. Off-Site Backup 2
5.2. PROCEDURAL CONTROLS 2
5.2.1. Trusted roles 2
5.2.2. Number of persons required per task 2
5.2.3. Identification and authentication for each role 2
5.3. PERSONNEL SECURITY CONTROLS 2
5.3.1. Background, qualifications, experience and clearance requirements 2
5.3.2. Background check procedures 2
5.3.3. Training requirements 2

5.3.4. Retraining frequency and requirements 2
5.3.5. Job rotation frequency and sequence 2
5.3.6. Sanctions for unauthorised actions 2
5.3.7. Contracting personnel requirements 2
5.3.8. Documentation supplied to personnel 2

6. TECHNICAL SECURITY CONTROLS 2

6.1. KEY PAIR GENERATION AND INSTALLATION 2
6.1.1. Key pair generation 2
6.1.2. Private Key delivery to entity 2
6.1.3. Public Key delivery to certificate issuer 2
6.1.4. CA Public Key delivery to users 2
6.1.5. Key sizes 2
6.1.6. Public Key parameters generation 2
6.1.7. Parameter quality checking 2
6.1.8. Hardware/software key generation 2
6.1.9. Key usage purposes 2
6.2. PRIVATE KEY PROTECTION 2
6.2.1. Standards for cryptographic module 2
6.2.2. Private key (n out of m) multi-person control 2
6.2.3. Private key escrow 2
6.2.4. Private key backup 2
6.2.5. Private key archival 2
6.2.6. Private key entry into cryptographic module 2
6.2.7. Method of activating private key 2
6.2.8. Method of deactivating private key 2
6.2.9. Method of destroying private key 2
6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT 2
6.3.1. Public key archival 2
6.3.2. Usage periods for the public and private keys 2
6.4. ACTIVATION DATA 2
6.4.1. Activation data generation and installation 2
6.4.2. Activation data protection 2
6.5. COMPUTER SECURITY CONTROLS 2
6.5.1. Specific computer security technical requirements 2
6.5.2. Computer security rating 2
6.6. LIFE CYCLE TECHNICAL CONTROLS 2
6.6.1. System development controls 2
6.6.2. Security management controls 2

6.6.3. Life cycle security ratings 2
6.7. NETWORK SECURITY CONTROLS 2
6.8. CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 2
7. CERTIFICATE AND CRL PROFILES 2
7.1.1. Version number(s) 2
7.1.2. Certificate extensions 2
7.1.3. Algorithm object identifiers 2
7.1.4. Name forms 2
7.1.5. Name constraints 2
7.1.6. Certificate policy object identifier 2
7.1.7. Usage of policy constraints extension 2
7.1.8. Policy qualifiers syntax and semantics 2
7.1.9. Processing semantics for the critical certificate policy extension 2
7.2. CRL PROFILE 2
8. SPECIFICATION ADMINISTRATION 2
8.1. SPECIFICATION CHANGE PROCEDURES 2
8.2. PUBLICATION AND NOTIFICATION POLICIES 2
8.2.1. CP Publication and Notification 2
8.3. CPS / CP APPROVAL PROCEDURES 2

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 used for Bank of China (Hong Kong) Limited ("BOCHK"). It describes the practices and procedures involved in the issuance of public key digital certificates by Digi-Sign's "general purpose" PKI hierarchy to the organization or individual who has enrolled or has applied to enrol for services provided by BOCHK or its associate companies . Such digital certificate is known as "BOC Corporate e-Certificate" in this document.

1.2. Policy Identification

1.2.1. Certificate Policy (CP) Identification

This CP has been allocated the OID: 1.3.6.1.4.1.8420.15.1.0, 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
15	BOCHK 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 Registration Authority (RA) as stated in section 1.3.3. of this CP.
- Subscribers, as stated in section 1.3.4 of this CP.

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 within its certificate policy domains. Under this CP, the Digi-Sign CA will issue BOC Corporate e-Certificates to Registered Users of BOCHK and/or its associate companies.

Refer to Section 1.3.4 for definition of Registered Users.

1.3.3. Registration Authority (RA)

The Registration Authority (RA), whose functions are performed by BOCHK, 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 verifying the identity of Subscriber's Authorised Representatives, obtaining evidence of identity, registering Subscribers and records retention are to be performed by RA.

Refer to Section 1.3.4 for definition of Authorised Representatives.

1.3.4. Subscribers

Subscribers under this CP are Registered Users. Registered Users are defined as organisation or individual who has enrolled or has applied to enrol for services provided by the BOCHK and/or its associate companies. Subscribers can assign representative ("Authorised Representative") to sign, on behalf of the Subscriber, all documents relating to the application, use and revocation of the certificate issued under this CP. Subscriber can authorize users ("Authorised User") to use the key and certificate issued by the CA to the Subscriber under this CP. .

1.3.5. Relying Parties

The only parties authorized to rely on these certificates are BOCHK and its corresponding customers, or BOCHK's associate companies and their corresponding customers.

1.3.6. Applicability

1.3.6.1. General Purpose

These certificates are to be used exclusively for the services provided by BOCHK or its associate companies.

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 BOCHK.

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 Subscribers. 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 BOCHK 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 (RA) Obligations

BOCHK shall perform the Registration Authority (RA) function for the Digi-Sign CA under this CP. Whenever the term RA appears in this CP, it refers to BOCHK performing the RA functions. As RA, BOCHK accepts the following obligations:

- Receiving and processing certificate applications including obtaining evidence of organization identity and certificate applications information and accepting or rejecting applications
- Informing Subscribers of their obligations, including their duty to safeguard their private keys and promptly report any compromise or suspected compromise
- Submitting certificate requests that match with the information known to the RA at time of submission, and that are free from data entry errors
- Keeping such registration records during the validity of the relevant certificate
- Ensuring that Subscribers execute the relevant documents in the form approved by Digi-Sign and BOCHK, which approval shall not be unreasonably withheld or delayed by either Digi-Sign or BOCHK
- Complying with all notices, instructions and manuals (contents of such documents shall not contradict or be inconsistent with the provisions of this CP, the associated CPS, and the Digi-Sign General Purpose Certificate Service Agreement) issued by Digi-Sign from time to time
- Complying with this CP, the associated CPS and the Digi-Sign General Purpose Certificate Service Agreement
- Indemnifying Digi-Sign against any actual direct costs reasonably incurred by Digi-Sign to the extent attributable to RA's 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 BOCHK nor Digi-Sign shall be responsible for authentication of the identity of any Authorised Users 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 BOCHK or its associate companies. Subscriber obligations include:

- Understand and comply with all directions from BOCHK and/or its associate companies when using the certificate and the private key;
- Use the certificate and the private key strictly in accordance with this CP, the CPS and the Subscriber Terms and Conditions;
- Provide true and correct information upon applying for key and certificate and notify RA immediately of any changes thereafter;
- Notify RA 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 RA to revoke the certificate, or has been notified by RA 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 any third party; or
  - Assign any rights under the Subscriber Terms and Conditions or other applicable contract.
- Indemnify Digi-Sign, and/or BOCHK against any actual direct costs reasonably incurred by Digi-Sign and/or BOCHK to the extent 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 section 2.6 of this CP, which shall prevail over the provisions in the CPS in case of conflict.

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.
- Agree that no implied or express warranties are given by Digi-Sign or by any other entity (including without limitation, Bank of China (HK) Ltd. (BOCHK) as the RA) 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

2.2. Liability

The warranties expressly specified in:

- the *Digi-Sign General Purpose Certificate Service Agreement* between Digi-Sign and BOCHK, 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 BOCHK. 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.

In the absence of any documented contractual relationship between the CA and a Subscriber and/or relying party, Digi-Sign or BOCHK 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 BOCHK 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 RA

Subject to section 2.2 of this CP, BOCHK and Digi-Sign shall indemnify and at all time keep each other fully indemnified for all loss and damage suffered to the extent 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 and/or BOCHK fully indemnified for all loss and damage suffered by Digi-Sign and/or BOCHK resulting from:

- all breach, non-compliance or non-observance of the terms and conditions in this CP, the CPS or the Subscriber Terms and Conditions by the Subscriber; 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 or BOCHK an agent, fiduciary, trustee, or other representative of any Subscriber, 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 shall be construed in accordance with the laws of the Hong Kong SAR and the parties unconditionally and irrevocably submit to the non-exclusive jurisdiction of the courts of the 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. The parties reserve the right to resolve disputes through litigation in the courts of the Hong Kong SAR.

2.5. Fees

BOCHK shall pay Digi-Sign the fees specified in the *Digi-Sign General Purpose Certificate Service Agreement* between Digi-Sign and BOCHK, 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

Certificates will not be published in any public 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 every four hours' intervals each day in the manner as specified in section 4.4.9 of this CP.

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 RA 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 Certificate 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 Subscriber’s Authorized User]

OU = [Subscriber’s Name]

OU = [Subscriber’s Registration Number]

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

O = [Bank of China or associate company]

C = HK

3.1.2. Need for names to be meaningful

Names used within the BOC Corporate e-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

The BOC Corporate e-Certificate 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 and shall have been approved by BOCHK before submission to Digi-Sign.

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

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 and BOCHK 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

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 the Subscriber, and this will be done in a secure manner. As all keys are centrally generated, there is no requirement for the Subscriber to prove possession of the private key.

3.1.8. Authentication of organization identity

Authentication of organization identity is the responsibility of the RA. 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

No authentication of individual identity of the Authorised Users will be conducted by Digi-Sign or BOCHK. The Subscribers shall be solely responsible for the authentication of the identity of individual Authorised Users nominated by them and ensuring that the information of such Authorised Users provided to Digi-Sign and BOCHK 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 Authorised Users who make use of the certificate with or without the authority of such Subscribers. Digi-Sign and BOCHK 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 Authorised Users or the other party/parties of such Subscribers.

For the avoidance of doubt, neither BOCHK nor Digi-Sign shall be responsible for the authentication of the identity of any Authorised Users of any Subscribers.

3.2. Certificate Renewal

Digi-Sign will issue a new BOC Corporate e-Certificate for Subscriber to replace the expired one during certificate renewal. Upon receipt of certificate renewal request submitted by BOCHK, 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 an existing certificate is due to expire, Digi-Sign will issue an expiry notice to BOCHK not less than 2 months before the expiry date of the certificate. BOCHK will assist the Subscriber to submit certificate renewal request, and this should be done before the existing certificate expiry date.

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

Upon approval of the certificate renewal, 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, 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

The Subscriber warrants to Digi-Sign and BOCHK that the information provided is true and correct, and must provide further proof to substantiate this information upon request by Digi-Sign and BOCHK.

Upon submitting a Subscriber application form, BOCHK warrants to Digi-Sign that the information provided in the application form matches with the incorporation or identity documents provided by the Subscribers, and when requested to do so by Digi-Sign, shall requests further information or documents from the Subscribers in order that Digi-Sign may approve the application and generate the required Key. .

It is the responsibility of BOCHK to deliver the Subscriber application form lodged by the Subscribers to Digi-Sign, Digi-Sign will undertake to notify BOCHK 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.

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 BOCHK. 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 Subscriber's receipt of a certificate and its subsequent use of its keys and certificates. By accepting a certificate, the Subscriber:

- agrees to be bound by the continuing responsibilities, obligations and duties imposed on it by the Subscriber Terms and Conditions, the applicable CPS and this CP
- warrants that to its knowledge no unauthorised person has had access to the private key associated with the certificate
- represents that the certificate information it has supplied during its registration is true and has been accurately and fully published within the certificate
- undertakes to inform BOCHK and Digi-Sign immediately if its information has changed or is known to be about to change.

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
- BOCHK 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 law;

(2) It is determined in the reasonable opinion of Digi-Sign 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 and the Subscriber Terms and Conditions;
- 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 organisation's assets;
- a director, or officer, or member of the senior management of the Subscriber organisation 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 BOCHK 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 BOCHK

BOCHK may at any time apply to Digi-Sign to revoke a certificate. However, BOCHK 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

BOCHK may request to revoke a certificate by sending the revocation request to Digi-Sign a) by fax on a prescribed form, or b) by post on a prescribed form or c) by digitally signed email.

The times to receive the revocation request are:

Monday to Friday:	8:30am to 4:00pm
Saturday:	8:30am to 10:00am

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

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 same working day of its receipt at the Digi-Sign office. Processing of the request will include checking of the BOCHK's authorised signature in the revocation request.

Once the validity of the revocation request is established, Digi-Sign will initiate action in its system to revoke the certificate, and update the CRL.

However, BOCHK may in an emergency situation notify Digi-Sign of its intention to revoke a certificate by telephone (Refer to the Emergency Telephone Number provided in CPS). Upon receipt of such telephone notification, Digi-Sign will temporarily suspend the relevant certificate, but will not proceed to revoke the certificate. BOCHK then will send its revocation request on the prescribed form to Digi-Sign's office within 2 working days after the telephone notification. Digi-Sign will revoke the certificate in accordance with section 4.4 upon receipt of the revocation request. If Digi-Sign fails to receive the revocation request within 2 working days after receiving the faxed-in or email notification, Digi-Sign will lift the suspension so that use of the certificate may resume. Digi-Sign shall suspend the certificate within 8 hours from the receipt of the telephone notification. If BOCHK or the Subscriber needs assistance, it may call the Digi-Sign hotline specified in section 1.4.1 of the CPS.

The times to receive the emergency revocation request are:

Sunday/Public Holidays:	9:00am to 12:00 noon

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

Any revocation or emergency revocation notification received outside the hours as stated in this section 4.4.3 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 BOCHK revocation request form in soft copy.

(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 BOCHK, 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 the time specified in Section 4.4.3.

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

The issuing CA will use its best endeavors to publish a most updated CRL at every four hours' interval each day following the schedule below :

CRL Publication Time (HKG Time, i.e. GMT+8)	02:00	06:00	10:00	14:00	18:00	22:00

The issuing CA will use its best endeavors to inform BOCHK of any delay on CRL release, or any change of CRL issuance frequency initiated by the issuing CA.

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 Subscribers must be generated in a manner that ensures the private key is known only to the authorised custodian of the key pair. The CPS describes the use of a Hardware Security Module (HSM) for the generation of CA keys.

Keys for Subscribers are generated by Digi-Sign upon receipt of a Subscriber application form from BOCHK. 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

Prior to the delivery of the private key, the Subscriber will receive a pre-generated PIN Mailer from BOCHK upon submission of application form.

Upon generation of the private keys, the private keys will be stored in a storage medium (floppy diskette; or smart USB token upon request of Subscriber specified in the Subscriber application form), which will be sealed in an individual secure packet for delivery. The secure packets will be delivered to the Subscriber by post or by delivery service offered by couriers or other delivery agents.

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 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 key generation, 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	(Optional) 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 bits.

Password based encryption algorithm for PKCS12,
pbeWithSHA1And40BitRC2_CBC(OID 1.2.840.113549.1.12.1.6)

7.1.4. Name forms

ELEMENT	X.521 ATTRIBUTE TYPE	VALUE	
		Issuer	Subject
Country	countryName	HK	HK
Organisation	organizationName	DIGI-SIGN CERTIFICATION SERVICES LIMITED	Bank of China or associate company
Organisational Unit	organizationalUnitName	BRN 31346952-000	1. SRN assigned by Digi-Sign 2. Subscriber's Registration Number 3. Subscriber's Name
Common Name	commonName	ID-CERT GENERAL SIGNING CA CERT	Name of Authorised User. Maximum of 50 characters

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 Subscribers of BOC Corporate e-Certificate 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 Subscribers include editorial corrections, typographical corrections, changes to contact details and any other change reasonably 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 Subscribers of BOC Corporate e-Certificates may be made if and only if Digi-Sign PAA and BOCHK 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 Subscribers include any change that affects the level of assurance or acceptability of related certificates. Material changes require the consent of the Digi-Sign PAA and BOCHK.

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 CP.