根據電子交易條例作為認可核證機關

之

香港互聯網註冊管理有限公司
數碼證書（個人）
數碼證書（機構）
數碼證書（保密）

核證作業準則

日期：2026 年 4 月 16 日
物件識別碼：1.3.6.1.4.1.64092.1.1.1

目錄

前言

香港法例第 553 章《電子交易條例》(「條例」) 列載公開密碼匙基礎建設（公匙基建）之法律架構。公匙基建利便電子交易作商業及其他用途。公匙基建由多個元素組成，包括法律責任、政策、硬體、軟件、資料庫、網絡及保安程序。

公匙密碼技術涉及運用一條私人密碼匙及一條公開密碼匙。公開密碼匙及其配對私人密碼匙在運算上有關連。電子交易運用公匙密碼技術之主要原理為：經公開密碼匙加密之信息只可用其配對私人密碼匙解密；和經私人密碼匙加密之信息亦只可用其配對公開密碼匙解密。

設計公匙基建之目的，為支援以上述方式在香港特別行政區進行商業活動及其他交易。

根據條例，核證機關可向數碼政策專員申請成為認可核證機關。認可核證機關可發出獲數碼政策專員根據條例第 22 條認可的證書，以及未獲認可的證書。香港互聯網註冊管理有限公司已決定申請成為認可核證機關，而就此文件而言，其身分為 **香港數碼證書頒發中心**。

目前，香港互聯網註冊管理有限公司已批出合約予翹晉電子商務有限公司（「合約」），根據本核證作業準則營運和維持香港數碼證書頒發中心的系統和服務。

根據合約，在得到香港互聯網註冊管理有限公司的書面同意後，翹晉電子商務有限公司可以委任合約分判商執行合約中的部份工作。**附錄 F** 列載翹晉電子商務有限公司的合約分判商之名單（若有的話）。在本核證作業準則內，「承辦商」是指翹晉電子商務有限公司及其合約分判商（若有的話）。

此外，香港數碼證書頒發中心可委任登記機構作為代理人，執行本準則所載認可核證機關的部分職能。登記機構名單（若有的話）載於**附錄 E**。

香港數碼證書頒發中心根據《電子交易條例》第 21 條及第 27 條仍為認可核證機關，而承辦商及登記機構乃根據條例第 33 條及《認可核證機關業務守則》第 3.2 條，由數碼政策專員發出之業務守則所委任的香港數碼證書頒發中心代理人。承辦商及登記機構亦能遵守與其運作相關的業務守則規定。

香港數碼證書頒發中心須對承辦商及登記機構在履行認可核證機關職能或提供服務時的行為及活動負責，尤其在發出及撤銷數碼證書方面。

香港數碼證書頒發中心作為認可核證機關，須根據條例使用穩當系統，以便在公開儲存庫內發出、暫時吊銷或撤銷及公布獲認可及接受的數碼證書，供安全的網上身分識別之用。根據本準則發出的數碼證書（個人）、數碼證書（機構）及數碼證書（保密）均屬條例下的認可證書，並於本準則中統稱為「證書」或「數碼證書」。

本核證作業準則列載數碼證書的實務守則，其結構如下：

第 1 條 載有概述及聯絡資料

1・ 引言

1.1 概述

本核證作業準則(「準則」)由香港互聯網註冊管理有限公司公布，使公眾有所瞭解，並規定香港互聯網註冊管理有限公司以香港數碼證書頒發中心身份在發出、暫時吊銷或撤銷及公布數碼證書時採用之做法及標準。

香港數碼證書頒發中心將維護本準則，以符合香港《電子交易條例》(第 553 章)及《認可核證機關業務守則》相關規例。

香港互聯網註冊管理有限公司已獲 Internet Assigned Numbers Authority (IANA) 分配私人企業號碼（Private Enterprise Number）64092 號。**「1.3.6.1.4.1.64092.1.1.1」**為本準則的物件識別碼（**Object Identifier, OID**）(見**附錄 B** 內關於核證政策（Certificate Policies）的說明）。

本準則列載參與香港數碼證書頒發中心所用系統之人士之角色、職能、義務及潛在責任。本準則列出核實證書(即根據本作業準則發出的證書)申請人身分的程序，並介紹香港數碼證書頒發中心之運作、程序及保安要求。

香港數碼證書頒發中心根據本準則發出之證書將得到倚據人士之倚據並用來核實數碼簽署。利用由香港數碼證書頒發中心發出之證書之各倚據人士須獨立確認基於公匙基建之數碼簽署乃屬適當及充分可信，可用來認證各倚據人士之特定公匙基建應用程序上之參與者之身分。

香港數碼證書頒發中心作為認可核證機關，**根據本核證作業準則而發出的數碼證書(個人)、數碼證書(機構)及數碼證書(保密)**，香港數碼證書頒發中心已指明為認可證書。對登記人及倚據人士而言，根據該條例香港數碼證書頒發中心在法律上有義務使用穩當系統，發出、暫時吊銷或撤銷及在可供公眾使用之儲存庫公布獲接受之認可證書。認可證書的內容不但準確，並根據條例載有法例界定之事實陳述，包括陳述此等證書為按照本準則發出者(下文詳述其定義)。香港數碼證書頒發中心委任代理人之事實並無減輕其使用穩當系統之義務，亦無變更數碼證書作為獲認可證書具有之特性。

附錄 D 載有根據本準則發出之數碼證書特點摘要。

1.2 社區及適用性

1.2.1 核證機關

根據本準則，香港數碼證書頒發中心履行核證機關之職能並承擔其義務。香港數碼證書頒發中心乃唯一根據本準則授權發出證書之核證機關（見第 2.1.1 條）。

1.2.1.1 香港數碼證書頒發中心所作之陳述

根據本準則而發出之證書，香港數碼證書頒發中心向根據本準則第 2.1.6 條及其他有關章條之倚據人士表明，香港數碼證書頒發中心已根據本準則發出證書。透過公布本準則所述之證書，香港數碼證書頒發中心即向根據本準則第 2.1.6 條及其他有關章條之倚據人士表明，香港數碼證書頒發中心已根據本準則發出證書予其中已辨識之登記人。

1.2.1.2 生效

香港數碼證書頒發中心將於儲存庫公布經由登記人接受並已發出之認可證書。（見第 2.5 條）

1.2.1.3 香港數碼證書頒發中心進行分包合約之權利

只要分包商同意與香港數碼證書頒發中心簽訂合約承擔有關職務，香港數碼證書頒發中心可把履行本準則及登記人協議之部分或全部工作之義務，批予分包商執行。無論有關職務是否批出由分包商執行，香港數碼證書頒發中心仍會負責履行本準則及登記人協議。

1.2.2 最終實體

根據本核證作業準則，存在兩類最終實體，包括登記人及倚據人士。登記人指於 附錄 A 內所指的「登記人」或「登記人機構」。倚據人士乃倚據香港數碼證書頒發中心發出之任何類別或種類證書，包括但不限於用於交易之數碼證書。特此澄清，倚據人士不應倚據代理機構或承辦商。香港數碼證書頒發中心透過其代理機構或承辦商發出數碼證書，而代理機構及承辦商對倚據人士並無任何謹慎職責，亦不需對倚據人士就發出數碼證書而負責（見第 2.1.2 及 2.1.3 條）。於交易中依據其他登記人之數碼證書之登記人乃為有關此證書之倚據人士。**請倚據人士留意，除特別聲明外，**香港數碼證書頒發中心**數碼證書系統並無年齡限制，未成年人仕可申請並領取數碼證書。**

1.2.2.1 登記人之保證及陳述

各申請人（如申請數碼證書（機構）及數碼證書（保密），獲授權代表會代表申請人）須接受本準則規定之條款，其中載有一條款，申請人據此條款同意，申請人一經接受根據本準則發出之證書，即表示其向香港數碼證書頒發中心保證（承諾）並向所有其他有關人士（尤其是倚據人士）作出陳述，在證書之有效期間，以下事實乃屬真實並將保持真實：

a) 除數碼證書（個人）登記人、數碼證書（機構）的授權用戶及數碼證書（保密）的授權單位外，並無其他人士曾取用登記人之私人密碼匙；
b) 使用與登記人數碼證書所載之公開密碼匙相關之登記人私人密碼匙所產生之每一數碼簽署實屬登記人之數碼簽署；
c) 數碼證書（保密）將只會用於第 1.2.3.3 條指明的用途；
d) 證書所載之所有資料及由登記人作出之陳述均屬真實；
e) 證書將只會用於符合本核證作業準則之認可及合法用途；
f) 在證書申請過程中所提供之所有資料，均並無侵犯或違反任何第三方之商標、服務標記、品牌、公司名稱或任何知識產權。

1.2.3 登記人之類別

根據本準則香港數碼證書頒發中心僅發出證書予其申請已獲香港數碼證書頒發中心批准並已以適當形式簽署或確定接受登記人協議之申請人士。三類數碼證書會根據本準則而發出：

1.2.3.1 數碼證書（個人）

根據本準則和登記人協議，數碼證書（個人）會發出予持有香港身份證人士。此等證書可用來從事商業經營。

數碼證書（個人）可發出予持有香港身份證之十八歲以下人士（另見第 3.1.1.2 條）。

1.2.3.2 數碼證書（機構）

數碼證書（機構）發給 (i) 香港特別行政區政府各政策局及部門、(ii) 獲香港特別行政區政府發出有效商業登記證或獲稅務局根據《稅務條例》（第 112 章）發出的有效證明文件的申報財務機構／申報實體，以及 (iii) 獲香港法例認可存在之本港法定團體（即「登記人機構」），並識別已獲該登記人機構授權使用該數碼證書（機構）私人密碼匙的成員或僱員（即「授權用戶」）。此等

證書與數碼證書（個人）之用途大致相同。

登記人機構（包括但不限於上述申報財務機構及申報實體）承諾，不會授權予授權用戶使用數碼證書（機構）於任何其他用途，除加密與解密電子信息，或於**附錄 H** 所指的特定應用程式內產生數碼簽署外。

1.2.3.3 數碼證書（保密）

數碼證書（保密）發給香港特別行政區政府各政策局及部門、獲香港特別行政區政府發出有效商業登記證之機構以及獲香港法例認可存在之本港法定團體（即「登記人機構」），並擬供已獲登記人機構授權使用數碼證書（保密）私人密碼匙之機構單位（“授權單位”）使用。

此類證書只可用作：

i) 傳送加密之數碼信息予登記人機構；
ii) 容許登記人機構為信息解密；及
iii) 容許登記人機構發出認收信息並附加其數碼簽署以證實其登記人機構收件身分，藉此確認已收訖送出之加密信息。

登記人機構向香港數碼證書頒發中心承諾，不會授權予授權單位使用此類證書之數碼簽署作其他用途。由此，利用此類證書私人密碼匙產生之數碼簽署如作為上文所述認收信息以外的用途，必須視為未經授權許可產生之簽署，此簽署亦必須視作未經授權之簽署。

登記人機構向香港數碼證書頒發中心承諾，不會授權予授權單位使用此類證書的數碼簽署作任何其他用途。由此，凡利用此類證書私人密碼匙產生之數碼簽署，如非用於上文所述認收信息，必須視為未經登記人機構授權而產生及使用之簽署，並必須視作未經授權之簽署。

1.2.4 證書之期限

證書的有效期由產生自香港數碼證書頒發中心系統當日起即日生效。

申請數碼證書時，申請人可自行選擇有效期。根據本核證作業準則發出予新申請人之證書，其可選擇的有效期如下：

證書類別	在證書內指明的有效期
數碼證書（個人）	一年、二年或三年
數碼證書（機構）	一年或二年
數碼證書（保密）	一年、二年或三年

根據本核證作業準則之證書續期程序而發出之證書有效期可超過上述之有效期(見第 3.3 及 3.4 條)。數碼證書內會註明其有效期。根據本準則發出之證書格式列於**附錄 B**。

1.2.5 官方網站及數碼證書登記人平台

香港數碼證書頒發中心透過其官方網站及數碼證書登記人平台提供服務，網址如下：

核證機關官方網站：https://www.hkca.hk
數碼證書登記人平台：https://www.hkca.hk/subscriber

所有首次申請及證書撤銷或到期後之申請，均視為新申請。此等申請必須透過數碼證書登記人平台遞交，並須由申請人使用「智方便+」成功完成認證。

網上申請程序將依據本核證作業準則第 3 及第 4 條指明的程序。

1.3 聯絡資料

登記人可經由以下途徑作出查詢、建議或投訴：

郵寄地址：香港數碼證書頒發中心，香港數碼港道 100 號數碼港 3 座 C 區 5 樓 501 室
電話：(852) 2319 2303　傳真：(852) 2319 2626
電郵地址 ：enquiry@hkca.hk

1.4 處理投訴程序

香港數碼證書頒發中心會盡快處理所有以書面及口頭作出的投訴，並在收到投訴後十天內給予詳細的答覆。若十天內不能給予詳細的答覆，香港數碼證書頒發中心會向投訴人作出簡覆。在可行範圍內，香港數碼證書頒發中心人員會於收到投訴後盡快以電話、電郵或信件與投訴人聯絡，確認收到有關投訴及作出回覆。

2． 一般規定

2.1 義務

香港數碼證書頒發中心對登記人之義務乃由本準則及與登記人以登記人協議形式達成之合約之條款進行定義及限制。無論登記人是否亦為有關其他登記人證書之倚據人士，均須如此。關於非登記人倚據人士，本準則知會該等人士，香港數碼證書頒發中心僅承諾採取合理技術及謹慎以避免在根據條例及本準則發出、暫時吊銷、撤銷、及公布證書時對倚據人士造成若干類型之損失及損害，並就下文及所發出之證書所載之責任限定幣值。

2.1.1 核證機關之義務

根據條例，香港數碼證書頒發中心為認可核證機關，負責使用穩當系統發出、暫時吊銷、撤銷、及利用公開儲存庫公布已獲登記人接受之認可證書。根據本準則，香港數碼證書頒發中心有下述義務：

a) 依時發出及公布證書（見第 2.5 條），
b) 通知申請人有關已批准或被拒絕的申請（見第 4.1 至 4.3 條），
c) 暫時吊銷或撤銷證書並依時公布證書撤銷清單（見第 4.5 條），及
d) 通知登記人有關已暫時吊銷或撤銷的證書（見第 4.5.1., 4.5.2. 及 4.5.3 條）。

2.1.2 核證登記機關之義務及責任

核證登記機關僅遵照與香港數碼證書頒發中心就獲其指定為代理人，代表其履行本準則詳述之若干義務而訂立之合約(代理人合約)之條款對香港數碼證書頒發中心負責。核證登記機關代表香港數碼證書頒發中心收集及保留根據本準則及登記人協議之條款所提供之文件及資料。香港數碼證書頒發中心須由始至終對其核證登記機關所執行或其本意是執行香港數碼證書頒發中心的功能、權力、權利和職責負責。

核證登記機關不為任何登記人協議之簽約方，亦不就發出、暫時吊銷或撤銷或公布數碼證書，或就收集及保留文件或資料對登記人或倚據人士承擔任何謹慎職責。核證登記機關之行為僅為代表香港數碼證書頒發中心履行香港數碼證書頒發中心於此等事項之義務及責任。核證登記機關有權代表香港數碼證書頒發中心實施登記人協議之條款（除非及直至該機關被撤銷及登記人正式獲通知任何該等撤銷）。**在任何情況下，核證登記機關不須就登記人協議或核證登記機關代表香港數碼證書頒發中心作為認可核證機關發出之證書對登記人或倚據人士承擔任何責任。**

2.1.3 承辦商之義務

承辦商祇會依據香港數碼證書頒發中心及承辦商之合約條款，包括承辦商作為香港數碼證書頒發中心所委任之代理人而須依據本作業守則建立、修改、提供、供應、交付、營運、管理、推廣及維持香港數碼證書頒發中心核證機關之系統及服務，而對香港數碼證書頒發中心負責。香港數碼證書頒發中心會依然對承辦商在其執行或將會執行香港數碼證書頒發中心之功能權力，權利及職能之行為負責。

2.1.4 登記人之義務

登記人負責：

a) 同意香港數碼證書頒發中心，在其處所內使用穩當的系統，在安全的環境下代表登記人製作配對密碼匙（就申請數碼證書（個人）、數碼證書（機構）或數碼證書（保密）而言）。
b) 妥善完成申請程序，並確認接受登記人協議（申請數碼證書（機構）或數碼證書（加密）時，由獲授權代表執行），包括透過「智方便+」進行數碼簽署，履行該協議規定其應承擔之義務

及確保在申請證書時所作的陳述準確無誤。

c) 確認數碼證書、私人密碼匙及數碼證書密碼會以安全電子方式傳送：
   i. 私人密碼匙及相應的數碼證書可透過登記人平台使用登記人已註冊帳戶下載；申請數碼證書（機構）或數碼證書（保密）時，下載須透過獲授權代表的註冊帳戶進行。
   ii. 數碼證書密碼會以安全的一次性下載連結分開傳送至登記人註冊電郵；申請數碼證書（機構）時，連結會傳送至授權用戶的註冊電郵；申請數碼證書（保密）時，則傳送至授權單位的註冊電郵。
d) 妥善管理上述數碼證書，並確保下載連結及密碼的保密性。
e) 依據本準則所載程序，正確處理證書到期事宜。
f) 確認並承擔保護私人密碼匙機密性及完整性的責任，採取合理措施防止遺失、洩露或未經授權使用，並承擔因私人密碼匙洩露所引致的一切後果。
g) 一旦發現私人密碼匙遺失或洩露，須立即通知香港數碼證書頒發中心（洩露指資訊可能遭未經授權存取，導致未經授權披露、修改或使用）。
h) 即時通知香港數碼證書頒發中心任何證書資料或授權用戶資料的變更。
i) 即時通知香港數碼證書頒發中心任何與獲授權代表任命或資料有關的變更（適用於數碼證書（機構）、數碼證書（保密））。
j) 在登記人明確知曉香港數碼證書頒發中心根據準則條款可能據以暫時吊銷或撤銷證書之任何事項之情況下，或登記人已作出撤銷申請或經香港數碼證書頒發中心知會，香港數碼證書頒發中心擬根據本準則之條款暫時吊銷或撤銷證書後，均不得在交易中使用證書。
k) 在明知香港數碼證書頒發中心可能據以暫時吊銷或撤銷證書之任何事項之情況下，或登記人作出撤銷申請或經香港數碼證書頒發中心知會擬暫時吊銷或撤銷證書時，須立即通知從事當時仍有待完成之任何交易之倚據人士，用於該交易之證書須予暫時吊銷或撤銷(由香港數碼證書頒發中心或經登記人申請)，並明確說明，因情形乃屬如此，故倚據人士不得就交易而倚據證書。
l) 同意其透過獲發出或接受證書向香港數碼證書頒發中心保證(承諾)並向所有倚據人士表明，在證書之有效期間，以上第 1.2.2.1 條載明之事實乃屬真實並將一直保持真實。
m) 用於身份鑒別的證書，其私人密碼匙只可以在證書有效期內使用。
n) 在明知香港數碼證書頒發中心可能據以暫時吊銷或撤銷證書之任何事項之情況下，或登記人作出撤銷申請或經香港數碼證書頒發中心知會擬暫時吊銷或撤銷證書時，須立即通知從事當時仍有待完成之任何交易之倚據人士，用於該交易之證書須予暫時吊銷或撤銷(由香港數碼證書頒發中心或經登記人申請)，並明確說明，因情形乃屬如此，故倚據人士不得就交易而倚據證書。
o) 承認知悉一經遞交數碼證書申請表，即授權向其他人或在香港數碼證書頒發中心儲存庫公布其數碼證書。
p) 用於身份鑒別的證書，其私人密碼匙只可以在證書有效期內使用。

數碼證書（保密）登記人亦負責確保：

- 獲授權使用者只獲登記人機構授權使用證書以及有關之數碼簽署，以解密並認收對方送來加密之電子信息，不得作其他用途；
- 此等證書只可用以(i)向登記人傳送加密電子信息，(ii)容許登記人機構為信息解密，以及(iii)容許登記人機構發出認收信息並附加其數碼簽署以證實其登記人機構收件身分，藉此確認送出之加密信息已經收訖；
- 不會試圖使用數碼證書(保密)的私人密碼匙以產生數碼簽署並用作認收信息以外用途；及
- 獲授權使用者採取合理預防措施以維護私人密碼匙之安全。

2.1.5 登記人之責任

各登記人承認，若上述義務未得以履行，則根據登記人協議及/或法例，各登記人有或可能有責任向香港數碼證書頒發中心及/或其他人士(包括倚據人士)就可能因此產生之責任或損失及損害賠償損失。

2.1.6 倚據人士之義務

倚據數碼證書之倚據人士負責：

a) 倚據人士於依賴證書時如考慮過所有因素後確信倚據證書實屬合理，方可依賴該等證書。
b) 於倚據該等證書前，確定證書之使用及其證明的任何數碼簽署乃適合本準則規定之用途，而承辦商或核證登記機關（若有的話）(見**附錄 E**)並不對倚據人士承擔任何謹慎職責。
c) 於倚據證書前查核證書撤銷清單上之證書狀態。
d) 執行所有適當證書路徑認可程序。
e) 於證書有效期屆滿後，僅公開密碼匙還可以在簽名驗證時繼續使用。

2.2 其他規定

香港數碼證書頒發中心對登記人及倚據人士之義務

2.2.1 合理技術及謹慎

香港數碼證書頒發中心謹此與各登記人協議，根據本準則香港數碼證書頒發中心、承辦商及代表香港數碼證書頒發中心之核證登記機關向各登記人及倚據人士履行及行使作為核證機關所具之義務和權利時，採取合理程度之技術及謹慎。香港數碼證書頒發中心不向登記人或倚據人士承擔任何絕對義務。**香港數碼證書頒發中心不保證香港數碼證書頒發中心、承辦商或代表香港數碼證書頒發中心之核證登記機關根據本準則提供之服務不中斷或無錯誤或比香港數碼證書頒發中心、其職員、僱員或代理人行使合理程度之技術及謹慎執行本準則時應當取得之標準更高或不同。**

換言之，儘管香港數碼證書頒發中心、承辦商或代表香港數碼證書頒發中心之核證登記機關於執行本合約及其根據準則行使應有之權利及義務時採取合理程度之技術及謹慎，若登記人作為準則定義下之登記人或倚據人士、或非登記人的倚據人士，而遭受出自準則中描述之公開密碼匙基礎建設或與之相關任何性質之債務、損失或損害，包括隨後對另外一登記人證書之合理倚據而產生之損失或損害，各登記人及各倚據人士同意香港數碼證書頒發中心、承辦商及任何核證登記機關無需承擔任何責任、損失或損害。

即如香港數碼證書頒發中心、承辦商或代表香港數碼證書頒發中心之核證登記機關已採取合理程度之技術及謹慎之前提下，若登記人或倚據人士因倚據另一登記人由香港數碼證書頒發中心所發出之認可證書支援之虛假或偽造之數碼簽署而蒙受損失或損害，香港數碼證書頒發中心、承辦商或代表香港數碼證書頒發中心之核證登記機關概不負責。

亦即如在香港數碼證書頒發中心（承辦商或代表香港數碼證書頒發中心之核證登記機關）已採取合理程度之技術或謹慎以避免及/或減輕無法控制事件後果之前提下，若登記人或倚據人士因香港數碼證書頒發中心不能控制之情況遭受不良影響，香港數碼證書頒發中心、承辦商或任何核證登記機關概不負責。香港數碼證書頒發中心控制以外之情況包括但不限於互聯網或電訊或其他基礎建設系統之可供使用情況，或天災、戰爭、軍事行動、國家緊急狀態、疫症、火災、水災、地震、罷工或暴亂或其他登記人或其他第三者之疏忽或蓄意不當行為。

2.2.2 非商品供應

特此澄清，登記人協議並非任何性質商品之供應合約。任何及所有據此發出之證書持續為香港數碼證書頒發中心之財產及為其擁有且受其控制，證書中之權利、所有權或利益不得轉讓於登記

人，登記人僅有權申請發出證書及根據該登記人協議之條款倚據此證書及其他登記人之證書。因此，該登記人協議不包括（或不會包括）明示或暗示關於證書為某一特定目的之可商售性或適用性或其他適合於商品供應合約之條款或保證。同樣地，香港數碼證書頒發中心在可供倚據人士接達之公開儲存庫內提供之證書，並非作為對倚據人士供應任何商品；亦不會作為對倚據人士關於證書為某一特定目的之可商售性或適用性的保證；亦不會作為向倚據人士作出供應商品的陳述或保證。香港數碼證書頒發中心雖同意將上述物品轉讓予申請人或登記人作本準則指定用途；但亦合理謹慎確保此等物品適合作本準則所述完成及接受證書之用途。若未能履行承諾，香港數碼證書頒發中心須承擔下文第 2.2.3-2.2.4 條所述責任。另外，由香港數碼證書頒發中心轉讓的物品可內載其他與完成及接受數碼證書無關之資料。若確實如此，與此等資料有關之法律觀點並非由核證作業準則或登記人協議規管，而須由物品內另行載述之條文決定。

2.2.3 法律責任限制

2.2.3.1 限制之合理性

各登記人或倚據人士必須同意，香港數碼證書頒發中心按本登記人協議及準則所列條件限制其法律責任實屬合理。

2.2.3.2 可追討損失種類之限制

在香港數碼證書頒發中心違反：

a) 本登記人協議；或
b) 任何謹慎職責－尤其當登記人或倚據人士、或其他人、或以其他任何方式，倚據或使用香港數碼證書頒發中心根據公開密碼匙基礎建設而發出之任何證書時－應根據登記人協議，為登記人或倚據人士，而採取合理技巧及謹慎及/或職責；

的情況下，而登記人或倚據人士（無論作為根據準則或以其他任何方式定義之登記人或倚據人士）蒙受損失及損害，**香港數碼證書頒發中心概不負責關乎下述原因之賠償或其他補救措施：**

a) 任何直接或間接利潤或收入損失、信譽或商譽損失或傷害、任何商機或契機損失、失去項目、或失去或無法使用任何數據、設備或軟件；或
b) 任何間接、相應而生或附帶引起之損失或損害，而且即使在後者情況下，香港數碼證書頒發中心已獲提前通知此類損失或損害之可能性。

2.2.3.3 限額 -- 20 萬港元

除下文所述例外情況外，在香港數碼證書頒發中心違反：

a) 本登記人協議及核證作業準則條文；或
b) 任何謹慎職責－尤其當登記人或倚據人士、或其他人士、或以其他任何方式倚據或使用香港數碼證書頒發中心根據公開密碼匙基礎建設而發出之任何證書時－應根據登記人協議、本準則、或法例，為登記人或倚據人士，採取合理技巧或謹慎及/或職責；

之情況下，而登記人或倚據人士蒙受損失及損害（無論作為根據準則或以其他任何方式定義之登記人或倚據人士），對於任何登記人、或任何倚據人士（無論作為根據準則或以其他任何方式定義之登記人或倚據人士或以任何其他身分），香港數碼證書頒發中心所負法律責任限制於且任何情況下每份數碼證書（個人）、數碼證書（機構）或數碼證書（保密）不得超過 20 萬港元、或每份發出予未滿 18 歲人仕的數碼證書（個人）0（零）港元。

2.2.3.4 提出索償之時限

任何登記人或倚據人士如欲向香港數碼證書頒發中心提出索償，且該索償源起於或以任何方式

與發出、暫時吊銷、撤銷或公布任何證書相關，則應在登記人或倚據人士察覺其有權提出此等索償的事實之日起一年內、或透過行使合理努力其有可能清楚此等事實之日起一年內（若更早）提出。特此澄清，不知曉此等事實之法律重要性乃無關重要。一年期限屆滿時，此等索償必須放棄且絕對禁止。

2.2.3.5 香港數碼證書頒發中心、承辦商、核證登記機關及各自之人員

無論香港數碼證書頒發中心、承辦商或任何核證登記機關或其各自之任何職員、僱員或其他代理人均非登記人協議之簽約人，登記人及倚據人士必須向香港數碼證書頒發中心承認，就登記人及倚據人士所知，香港數碼證書頒發中心、承辦商或任何核證登記機關之任何職員、僱員或代理人（就任何出於真誠、並與香港數碼證書頒發中心履行本登記人協議或由香港數碼證書頒發中心作為核證機關發出之任何證書相關，而作出的行動或遺漏事項）均不會自願接受或均不會接受向登記人、或倚據人士擔負任何個人責任或謹慎職責；每一位登記人及倚據人士接受並將繼續接受此點，並向香港數碼證書頒發中心保證不起訴或透過任何其他法律途徑對前述任何關於該人出於真誠（不論是否出於疏忽）、並與香港數碼證書頒發中心履行本登記人協議或由香港數碼證書頒發中心作為核證機關發出之任何證書相關，而作出的行動或遺漏事項尋求任何形式之追討或糾正，並承認香港數碼證書頒發中心享有充分法律及經濟利益以保護香港數碼證書頒發中心及上述機構及個人免受此等法律行動。

2.2.3.6 蓄意之不當行為或個人傷亡之責任

任何因欺詐或蓄意之不當行為或個人傷亡之責任均不在本準則、登記人協議或香港數碼證書頒發中心發出之證書之任何限制或除外規定範圍內，亦不受任何此等規定之限制或被任何此等規定免除。

2.2.3.7 證書通知、限制及倚據限額

香港數碼證書頒發中心發出之證書須被認作已包括下列倚據限額及／或法律責任限制通知：

> *"香港數碼證書頒發中心職員及承辦商按香港數碼證書頒發中心之核證作業準則所載條款及條件適用於本證書之情況下，根據香港法例第 553 章電子交易條例作為認可核證機關發出本證書。*
>
> *因此，任何人士倚據本證書前均應閱讀適用於數碼證書的準則（可瀏覽 https://www.hkca.hk ）。香港特別行政區法律適用於本證書，倚據人士須提交因倚據本證書而引致之任何爭議或問題予香港特別行政區法庭之非專有司法管轄權。*
>
> *倘閣下為倚據人士而不接受本證書據以發出之條款及條件，則不應倚據本證書。*
>
> *香港數碼證書頒發中心（經承辦商及其各自職員、僱員及代理人）發出本證書，但無須對倚據人士承擔任何責任或謹慎職責（準則中列明者除外）。*
>
> *倚據人士倚據本證書前負責：*
>
> *a. 只有當倚據人士於倚據時所知之所有情況證明倚據行為乃屬合理及本著真誠時，方可倚據本證書；*
> *b. 倚據本證書前，確定證書之使用及其證明的任何數碼簽署就準則規定之用途而言乃屬適當；*
> *c. 倚據本證書前，根據證書撤銷清單檢查本證書之狀態；及*
> *d. 履行所有適當證書路徑認可程序。*

若儘管香港數碼證書頒發中心、承辦商、其各自職員、僱員或代理人已採取合理技術及謹慎，本證書仍在任何方面不準確或誤導，則香港數碼證書頒發中心長、香港數碼證書頒發中心承辦商、其各自職員、僱員或代理人對倚據人士之任何損失或損害概不承擔任何責任，在該等情況下根據條例適用於本證書之倚據限額為 0 港元。

若本證書在任何方面不準確或誤導，而該等不準確或誤導乃因香港數碼證書頒發中心、承辦商、其各自職員、僱員或代理人之疏忽所導致，則香港數碼證書頒發中心將就因合理倚據本證書中之該等不準確或誤導事項而造成之經證實損失向每名倚據人士支付最多 20 萬港元、或支付最多 0（零）港元（如該證書為發出予未滿 18 歲人仕的數碼證書（個人）），惟該等損失不屬於及不包括（1）任何直接或間接利潤或收入損失、信譽或商譽損失或傷害、任何商機或契機、失去工程或失去或無法使用任何數據、設備或軟件或（2）任何間接、相應而生或附帶引起之損失或損害，而且即使在後者情況下，香港數碼證書頒發中心已被提前通知此類損失或損害之可能性。在該等情況下根據條例適用於本證書之倚據限額為 20 萬港元、或 0（零）港元（如該證書為發出予未滿 18 歲人仕的數碼證書（個人）），而在所有情形下就第（1）及（2）類損失而言倚據限額則為 0 港元。

在任何情況下，香港數碼證書頒發中心、承辦商、其各自職員、僱員或代理人概不對倚據人士就本證書承擔任何謹慎職責。

索賠時限
任何倚據人士如擬向香港數碼證書頒發中心索賠，且該索償源起於或以任何方式與發出、暫時吊銷、撤銷或公布任何證書相關，則應在倚據人士知悉存在任何有權提出此等索償事實之日起一年內或透過行使合理努力彼等有可能知悉此等事實之日起一年內（若更早）提出。特此澄清，不知曉此等事實之法律重要性乃無關重要。一年期限屆滿時，此等索償必須放棄且絕對禁止。

倘本證書包含任何由香港數碼證書頒發中心、承辦商、其各自職員、僱員或代理人作出之故意或罔顧後果之失實陳述，則本證書並不就彼等對因合理倚據本證書中之失實陳述而遭受損失之倚據人士所應承擔之法律責任作出任何限制。

本文所載之法律責任限制不適用於個人傷害或死亡之（不大可能發生之）情形。”

2.2.4 香港數碼證書頒發中心對已獲接收但有缺陷之數碼證書所承擔之責任

儘管上文已列明香港數碼證書頒發中心承擔責任之限制，若登記人接收證書後發現，因證書內之私人密碼匙或公開密碼匙出現差錯，導致基於公匙基建預期之交易無法適當完成或根本無法完成，則登記人須將此情況立即通知香港數碼證書頒發中心，以便撤銷證書及（如願意接受）重新發出。或倘此通知已於接收證書後三個月內發出且登記人不再需要證書，則香港數碼證書頒發中心若同意確有此差錯將進行退款。倘登記人於接收證書三個月過後方將此類差錯通知香港數碼證書頒發中心，則費用不會自動退還，而由香港數碼證書頒發中心酌情退回。

2.2.5 登記人的轉讓

登記人不可轉讓登記人協議或證書賦予之權利。擬轉讓之行為均屬無效。

2.2.6 陳述權限

除非獲得香港數碼證書頒發中心授權，香港數碼證書頒發中心、承辦商或任何核證登記機關之代理人或僱員無權代表香港數碼證書頒發中心對本準則之意義或解釋作任何陳述。

2.2.7 更改
香港數碼證書頒發中心有權更改本準則，而無須發出預先通知(見第 8 條)。登記人協議不得作出更改、修改或變更，除非符合本準則中之更改或變更規定，或獲得香港數碼證書頒發中心之明確書面同意。

2.2.8 保留所有權
根據本準則發出之證書上所有資料之實質權利、版權及知識產權現屬香港數碼證書頒發中心所有，日後亦然。

2.2.9 條款衝突
倘本準則與登記人協議或其他規則、指引或合約有衝突，登記人、倚據人士及香港數碼證書頒發中心須受本準則條款約束，除非該等條款受法律禁止。

2.2.10 受信關係
香港數碼證書頒發中心、承辦商或代表香港數碼證書頒發中心之任何核證登記機關並非登記人或倚據人士之代理人、受信人、受託人或其他代表。登記人及倚據人士無權以合約或其他方式約束香港數碼證書頒發中心、承辦商或代表香港數碼證書頒發中心之任何核證登記機關承擔登記人或倚據人士之代理人、受信人、受託人或其他代表之責任。

2.2.11 相互核證
香港數碼證書頒發中心根據本核證作業準則而發出的數碼證書（個人）、數碼證書（機構）及數碼證書（保密），在所有情形下均保留與另一家核證機關定義及確定適當理由進行相互核證之權利。

2.2.12 有關本核證作業準則與 RFC3647 標準制定電子認證業務規則的內容比較
本核證作業準則乃根據 RFC2527 標準而建構。考慮到登記人、倚據人士及其他相關人士已採用現行核證作業準則的格式並理解其內容達一段長時間，如為配合 RFC3647 標準而對目前應用的準則結構作出重大修訂，可能會令登記人、倚據人士及其他相關人士對本核證作業準則的內容產生混淆。有鑒於此，目前決定提供一份 依據 RFC3647 核證作業準則概要與本核證作業準則相關章節的比較表，載於 **附錄 I**，以供參考。

2.2.13 財務責任
保單已經備妥，有關證書之潛在或實質責任以及對倚據限額之索償均獲承保。

2.3 解釋及執行（管轄法律）

2.3.1 管轄法律
本準則受香港特別行政區法律規管。登記人及倚據人士同意受香港特別行政區法庭之非專有司法管轄權囿制。

2.3.2 可分割性、保留、合併及通知
若本準則之任何條款被宣佈或認為非法、不可執行或無效，則應刪除其中任何冒犯性詞語，直至該等條款合法及可執行為止，同時應保留該等條款之本意。本準則之任何條款之不可執行性將不損害任何其他條款之可執行性。

2.3.3 爭議解決程序
香港數碼證書頒發中心關於本準則範圍內之事宜之決定為最終決定。如有索償，請送交下列地

址：

香港互聯網註冊管理有限公司
香港數碼港道 100 號數碼港 3 座 C 區 5 樓 501 室
電郵地址 ：enquiry@hkca.hk

2.3.4 詮釋
本準則中英文本措詞詮釋若有歧異，以英文本為準。

2.4 登記費用

香港數碼證書頒發中心可不時釐定處理新申請及續期申請、撤銷請求、行政工作及其他與 數碼證書相關服務之收費。選用的儲存媒體或交付安排，或須繳付額外費用。 最新收費表載於香港數碼證書頒發中心網站。香港數碼證書頒發中心保留絕對權力，不時修訂相關收費表，並可透過其他方式發布。

除非獲香港數碼證書頒發中心豁免，登記人必須於每個登記期開始前（見第 3.2 節）全數繳付所有適用費用。倘若數碼證書的登記期於證書所列明的有效期內終止（亦見第 4.5.1.4(f) 節），香港數碼證書頒發中心可暫停或撤銷該數碼證書。

2.5 公布資料及儲存庫

根據條例之規定，香港數碼證書頒發中心維持一儲存庫，內有根據本核證作業準則發出並已經由登記人接受的證書清單、最新證書撤銷清單、香港數碼證書頒發中心公開密碼匙、本準則文本一份以及與本準則的數碼證書有關之其他資料，包括可於核證機關網站及數碼證書登記人平台取得的《登記人條款及條件》。本準則以及最新版本的《登記人條款及條件》將構成公開的登記人協議以及倚據人士協議。香港數碼證書頒發中心會及時發佈及更新儲存庫中有關披露文件，以及先前已發佈文件及其修訂的披露記錄。除平均每週兩小時之定期維修及任何緊急維修外，儲存庫基本上保持每日 24 小時、每週 7 日開放。香港數碼證書頒發中心會把按本準則經由登記人接受並發出予登記人的每張數碼證書，盡快於儲存庫內公布。儲存庫可透過下述 URL 接達：

https://www.香港數碼證書頒發中心.hk
ldap://ldap1.香港數碼證書頒發中心.hk

2.5.1 證書儲存庫控制
儲存庫所在位置可供在線瀏覽，並可防止擅進。

2.5.2 證書儲存庫進入要求
經授權之香港數碼證書頒發中心人士方可進入儲存庫更新及修改內容。在運行及管理儲存庫時，香港數碼證書頒發中心不會進行任何對倚據儲存庫（包括證書和其他信息）的人士造成不合理風險的活動。

2.5.3 證書儲存庫更新週期
每份證書一經登記人接受及發出後，以及如更新證書撤銷清單等其他相關情況時，儲存庫會盡快作出更新。

2.5.4 核准使用證書儲存庫內的資料

證書儲存庫內的資料，包括個人資料，會按照條例之規定且在符合方便進行合法電子交易或通訊之目的下作出公布。

2.6 遵守規定之評估

須根據條例以及認可核證機關守則之規定，至少每 12 個月進行一次遵守規定之評估，檢視香港數碼證書頒發中心發出、暫時吊銷或撤銷及公布證書之系統是否妥善遵守本準則。

2.7 機密性

在履行與香港數碼證書頒發中心發出、暫時吊銷、撤銷及公布數碼證書之有關任務時可取閱任何紀錄、書刊、紀錄冊、登記冊、通訊、資訊、文件或其他物料之香港數碼證書頒發中心、其人員、承辦商、核證登記機關及任何香港數碼證書頒發中心分包商之人員，不得向他人披露、不得允許或容受向他人披露載於該等紀錄、書刊、紀錄冊、登記冊、通訊、資訊、文件或其他物料內與另一人有關的任何資料。

香港數碼證書頒發中心會確保香港數碼證書頒發中心、承辦商、核證登記機關及任何香港數碼證書頒發中心分包商之人員，均會依循本分節所載之限制。作為根據本準則申請數碼證書之組成部分而提交之登記人資料，只會用於收集資料之目的，並以機密方式保存；惟在香港數碼證書頒發中心或承辦商為履行香港數碼證書頒發中心於本準則下的責任而有需要的情況下，則不在此限。除非經法庭發出之傳訊令或命令要求，或香港特別行政區的法律另有規定，否則未經登記人事先同意，不得將該等資料對外發佈。

3． 鑑別及認證

香港數碼證書頒發中心負責制訂核實數碼證書的新申請及續期申請的要求，以及其後的撤銷申請。香港數碼證書頒發中心保留其絕對權利，可在毋須提供任何解釋或理由的情況下，批准或拒絕任何數碼證書的新申請或續期申請，以及撤銷申請。

3.1 首次申請

所有申請人必須透過數碼證書登記人平台，或在適用的情況下，透過承辦商或核證登記機關，提交其數碼證書申請（見**附錄 E**）。

香港數碼證書頒發中心會進行所需程序，以核實從數碼證書申請中所收到的資料：

- 就數碼證書（個人）申請而言：申請人的身分；
- 就數碼證書（機構）申請而言：申請人、授權代表及各授權用戶的身分，以及授權代表獲申請人授權的有效性；
- 就具自動交換資料功能的數碼證書（機構）申請而言：申請人、授權代表及各授權用戶的身分，以及授權代表獲申請人及各授權用戶授權的有效性；
- 就數碼證書（保密）申請而言：申請人及授權代表的身分，以及授權代表獲申請人授權的有效性。

就透過數碼證書登記人平台提交的數碼證書申請而言，香港數碼證書頒發中心將（在其他事項以外）核實以下各項：

- 就數碼證書（個人）而言：
  a) 申請人已使用「智方便+」於數碼證書登記人平台建立個人帳戶，並提供與其香港身分證一致的個人身分資料；
  b) 申請人已使用「智方便+」對證書申請作出數碼簽署。
- 就數碼證書（機構）及數碼證書（保密）而言：
  a) 機構的授權代表已使用「智方便+」於數碼證書登記人平台建立公司帳戶，並提供與其香港身分證一致的個人身分資料；
  b) 授權代表已使用「智方便+」對證書申請作出數碼簽署，而有關機構將被視為登記人。
- 香港數碼證書頒發中心將接納透過「智方便+」提供的身分驗證及數碼簽署，作為充分的身分證明。數碼證書（機構）中所列明的授權用戶，其身分驗證並非必須。於申請獲批准後，香港數碼證書頒發中心將備備數碼證書，並通知申請人有關的發出程序。

就透過承辦商或核證登記機關提交的數碼證書申請而言，香港數碼證書頒發中心將根據承辦商或核證登記機關所提供的資料，核實申請人的個人資料。香港數碼證書頒發中心保留其絕對權利，可在其認為有需要的情況下，要求申請人提供額外的資料或文件，尤以在個別情況下為核實及驗證申請人的個人身分之目的。

3.1.1 名稱類型

3.1.1.1 數碼證書（個人）
透過證書上的主體名稱（於**附錄 B** 內指明），包括登記人香港身份證上顯示之姓名，可識別數碼證書（個人）登記人之身分。登記人香港身份證號碼則以雜湊數值形式儲存於證書內(見**附錄 B**)。

3.1.1.2 向十八歲以下登記人發出數碼證書(個人)
透過第 3.1.1.1 條內說明之證書上的主體名稱及”d-Cert (Personal/Minor)”字樣（見**附錄 B**），可識別登記人之身分，及顯示登記人獲發出證書時未滿 18 歲。

3.1.1.3 數碼證書（機構）
透過證書上的主體名稱（於**附錄 B** 內指明）可識別數碼證書（機構）登記人機構之身分，該名稱由以下資料組成：

a) 登記人機構在有關登記機關之登記名稱或香港特別行政區政府各政策局或部門或獲香港法例認可之本港法定團體名稱；如登記人機構為香港特別行政區政府各政策局或部門，則為該部門或政策局之正式名稱；及
b) 若登記人機構並非香港特別行政區政府各政策局或部門或香港法例認可存在之法定團體，則包括該機構之香港公司註冊/商業登記號碼，或該機構之稅務局參考編號。
c) 授權用戶香港身份證/護照上顯示之姓名；

3.1.1.4 數碼證書（保密）
透過證書上的主體名稱（於**附錄 B** 內指明）可識別數碼證書（保密）登記人機構之身分，該名稱由以下資料組成：

a) 登記人機構在有關登記機關之登記名稱或香港特別行政區政府各政策局或部門或獲香港法例認可之本港法定團體名稱；如登記人機構為香港特別行政區政府各政策局或部門，則為該部門或政策局之正式名稱；
b) 若登記人機構並非香港特別行政區政府各政策局或部門或香港法例認可存在之法定團體，則包括該機構之香港公司註冊/商業登記號碼；及
c) 登記人機構內授權單位之名稱。

3.1.1.5 獲授權代表
登記人機構獲授權代表雖替登記人機構辦理數碼證書（機構）或數碼證書（保密）之申請手續，然而該證書並不會辨識此獲授權代表身分。

3.1.1.6 機構中文名稱
數碼證書（個人）只用英文發出。

數碼證書（機構）用英文發出，但如登記人機構在申請表格上提供了中文名稱，該數碼證書將會包含其機構及分行中文名稱。如數碼證書（機構）之登記人機構僅有中文名稱，其機構英文名稱將被預設為「***CHINESE NAME ONLY***」。

數碼證書（保密）一律只用英文發出。如數碼證書（保密）之登記人機構僅有中文名稱或僅提供其中文名稱，該數碼證書將不會顯示其機構名稱。

3.1.2 名稱需有意義
所採用名稱之語義必須為一般人所能理解，方便辨識登記人身分。

3.1.3 詮釋各個名稱規則
香港數碼證書頒發中心數碼證書會載入之登記人名稱(主體名稱)類型見第 3.1.1 條。有關香港數碼證書頒發中心數碼證書主體名稱之詮釋應參照**附錄 B**。

3.1.4 名稱獨特性
對登記人而言，主體名稱 （於**附錄 B** 內指明）應無歧義而具獨特性。然而，此準則並不要求名稱某一特別部分或成分本身具獨特性或無歧義。

3.1.5 名稱申索爭議決議程序
香港數碼證書頒發中心可酌情處理有關名稱爭議之事宜並享有最終決定權。

3.1.6 侵犯及違反商標註冊
申請人及登記人向香港數碼證書頒發中心保證（承諾）並向倚據人士申述，申請證書過程提供之資料概無以任何方式侵犯或違反第三者之商標權、服務商標、商用名稱、公司名稱或知識產權。

3.1.7 證明擁有私人密碼匙之方法
香港數碼證書頒發中心為登記人提供代製密碼匙服務。香港數碼證書頒發中心在其處所內使用穩當的系統，在安全的環境下替登記人製作證書，以保證私人密碼匙不受干擾。

私人密碼匙連同相應的證書，將僅透過安全的網上渠道交付予登記人。於成功發出後，香港數碼證書頒發中心會向登記人發出兩（2）份獨立的電子通訊，詳列如下：

- 就數碼證書（個人）而言：
  a) 一則通知，讓登記人透過其已正式登記的個人帳戶下載證書及私人密碼匙，並以 PKCS#12 格式檔案封裝；
  b) 一條安全電子連結，用於取得密碼。該連結僅可使用一次，並會於發出日起一（1）個月後自動失效。

- 就數碼證書（機構）而言：
  a) 一則通知，讓登記人透過其已正式登記的公司帳戶下載證書及私人密碼匙，並以 PKCS#12 格式封裝；
  b) 一條安全電子連結，傳送至各授權用戶的指定電郵地址，用於取得該授權用戶的密碼。每條連結僅可使用一次，並會於發出日起一（1）個月後自動失效。

- 就數碼證書（保密）而言：
  a) 一則通知，讓登記人透過其已正式登記的公司帳戶下載證書及私人密碼匙，並以 PKCS#12 格式封裝；
  b) 一條安全電子連結，傳送至各授權單位的指定電郵地址，用於取得該授權單位的密碼。每條連結僅可使用一次，並會於發出日起一（1）個月後自動失效。

登記人成功完成（a）下載證書及私人密碼匙，以及（b）取得相關密碼後，香港數碼證書頒發中心將立即並永久從其系統中刪除私人密碼匙及密碼。此程序將構成以安全及可稽核方式擁有私人密碼匙的最終證明，並符合本準則第 4.1、4.2 及 4.3 條之規定。

3.1.8 機構申請人身分認證

3.1.8.1 數碼證書（機構）及數碼證書（保密）的機構申請人的身份認證將透過以下其中一個運作程序完成：

a) 申請人的授權代表將透過數碼證書登記人平台提交申請，並使用「智方便+」對該申請作出數碼簽署。
b) 申請人的授權代表將親身前往香港數碼證書頒發中心指明的處所，或香港數碼證書頒發中心所指明的承辦商或核證登記機關的處所，提交已正式填妥並簽署的數碼證書申請表及登記人協議，並出示其香港身分證或護照以作身分核驗。上述處所的工作人員將進行面對面核驗授權代表的身分，審閱並核證申請文件，然後將申請傳送至香港數碼證書頒發中心的處理中心作進一步處理。
c) 香港數碼證書頒發中心可全權酌情決定，在授權代表未親身到場的情況下接受申請文件，惟須符合以下條件：(1) 申請須附有授權代表的香港身分證或護照副本，並經授權代表正式簽署；及 (2) 同時符合以下兩項條件：
    i. 授權代表的身分已於登記人機構過往的申請中獲認證，且該授權代表曾於該過往申請中親身到訪香港數碼證書頒發中心指明的處所，或香港數碼證書頒發中心所指明的承辦商或核證登記機關的處所，以作身分核驗；及
    ii. 有合理理由重新確認授權代表的身分，包括但不限於透過與授權代表直接通話作確認，或將授權代表的簽署與過往申請所保存的紀錄作比對。
d) 香港數碼證書頒發中心保留權利，可在其全權酌情決定下，於對授權代表身分的真確性存有疑問時，拒絕任何申請。

3.1.8.2 每份數碼證書（機構）之申請須附有以下文件：
a) 蓋上申請機構 “For and on behalf of”（代表機構簽署）印章及附有該機構的獲授權簽署 之授權書。授權書註明該機構已授權有關人士 (即「獲授權代表」)代表該機構提交申請及識別列於數碼證書（機構）上的授權用戶；
b) 所有按此方式識別身分之授權用戶之香港身份證或護照副本。如授權用戶並非香港公民，亦可接受其提交有效旅遊證件的副本；
c) 由有關香港登記機關發出證明此機構確實存在之文件。有關文件的有效期由提交申請時起計，必須超過一個月。

3.1.8.3 每份數碼證書（保密）之申請須附有以下文件：
a) 蓋上申請機構 “For and on behalf of”（代表機構簽署）印章及附有該機構的獲授權簽署 之授權書。授權書註明該機構已授權有關人士 (即「獲授權代表」)代表該機構提交申請；
b) 由有關香港登記機關發出證明此機構確實存在之文件。有關文件的有效期由提交申請時起計，必須超過一個月。

3.1.8.4 香港特別行政區政府各政策局或部門之申請須附有蓋上該政策局或部門印鑑之便箋、信函或有關申請表格，指定獲授權代表以代表該政策局或部門簽署與申請、撤銷及續發香港數碼證書頒發中心數碼證書有關之所有文件。該便箋、信函或有關申請表格須由部門主任秘書或同級或上級人員簽署。

3.1.8.5　獲發出多於一年有效期數碼證書（機構）及數碼證書（保密）之登記人機構，香港數碼證書頒發中心會約於數碼證書有效期內每個週年日，再核對登記人機構的存在。如登記人機構的存在未能核實，香港數碼證書頒發中心可根據本準則第 4.5 條（暫時吊銷及撤銷證書）的條款暫時吊銷或撤銷發出予該登記人機構的證書。

3.1.9 個人申請人身分認證

各數碼證書（個人）申請人身分之確認將透過如下運作完成：

a) 申請人將透過數碼證書登記人平台提交申請，並使用「智方便+」對該申請作出數碼簽署。
b) 申請人將親身前往香港數碼證書頒發中心指明的處所，或香港數碼證書頒發中心所指明的承辦商或核證登記機關的處所，提交已正式填妥並簽署的數碼證書申請表及登記人協議，並出示其香港身分證或護照以作身分核驗。上述處所的工作人員將進行面對面核驗申請人的身分，審閱並核證申請文件，然後將申請傳送至香港數碼證書頒發中心的處理中心作進一步處理。
c) 申請人須出示其由有效的數碼證書（個人）支援的數碼簽署。
d) 香港數碼證書頒發中心保留權利，可在其全權酌情決定下，於對申請人身分的真確性存有疑問時，拒絕任何申請。

3.2 數碼證書續期

3.2.1 數碼證書（個人）續期

所有數碼證書登記人必須透過數碼證書登記人平台，或在適用情況下，透過承辦商或核證登記機關遞交其數碼證書續期申請（見**附錄 E**）。續期申請必須於證書屆滿日期前遞交，且在任何情況下不得遲於香港數碼證書頒發中心所訂明的最後期限，以避免證書有效性及相關服務中斷。

3.2.1.1　香港數碼證書頒發中心將於證書有效期屆滿前通知登記人續期其數碼證書（個人）。續期申請將透過數碼證書登記人平台提交。證書可於有效期屆滿前，按登記人要求並由香港數碼證書頒發中心酌情決定予以續期。續期申請的身分認證將透過「智方便+」進行數碼簽署。香港數碼證書頒發中心不會為已屆滿、暫停或撤銷的證書辦理續期。香港數碼證書頒發中心可全權酌情決定，將發出予登記人的新證書之有效期設定為比第 1.2.4 節所指明的有效期更長。

新證書有效期（附註 1）	新證書內指明的有效期開始日	新證書內指明的有效期屆滿日	備註
一年	新證書產生日期	原有證書（即須續期的證書）到期日之後一年	新的數碼證書的有效期可超過一年，但不會超過一年另一個月
二年	新證書產生日期	原有證書（即須續期的證書）到期日之後二年	新的數碼證書的有效期可超過二年，但不會超過二年另一個月
三年	新證書產生日期	原有證書（即須續期的證書）到期日之後三年	新的數碼證書的有效期可超過三年，但不會超過三年另一個月

附註：1. 參閱第 1.2.4 條

3.2.1.2　數碼證書（個人）不設自動續期。第 3.1.9 節所述的「個人申請人身分認證」程序通常適

用。然而，若續期申請是透過登記人平台提交，並由申請人使用「智方便+」進行數碼簽署（如第 3.1.9(a) 節所指明），或使用第 3.1.9(c) 節所指明的有效數碼簽署，則可在登記人毋須親身到場的情況下續期數碼證書（個人）。在所有其他情況下，登記人須向香港數碼證書頒發中心提交已正式填妥並簽署的證書續期申請表，以申請續期。續期申請程序的詳情載於香港數碼證書頒發中心網站。

3.2.1.3　於續期時，將透過香港數碼證書頒發中心的中央密碼匙製作服務產生新的密碼匙。原登記人協議的條款及條件將繼續適用於續期後的證書，如兩者有所抵觸，則以續期當日之核證作業準則內的條款為準。申請人應細閱續期當日有效的核證作業準則，方可遞交續期申請表。

3.2.2 數碼證書（機構）及數碼證書（保密）續期

3.2.2.1　香港數碼證書頒發中心會於證書的有效期屆滿前，向數碼證書（機構）及數碼證書（保密）登記人發出續期通知。證書可因應登記人的要求及香港數碼證書頒發中心的酌情權，在證書的有效期屆滿前獲得續期。香港數碼證書頒發中心不會為過期、已暫時吊銷或已撤銷的證書續期。因應香港數碼證書頒發中心的酌情權，發出給登記人的新證書的實際有效期會超過於第 1.2.4 條指明的證書有效期：

新證書有效期（附註 1）	新證書內指明的有效期開始日	新證書內指明的有效期屆滿日	備註
一年	新證書產生日期	原有證書（即須續期的證書）到期日之後一年	新的數碼證書的有效期可超過一年，但不會超過一年另一個月
二年	新證書產生日期	原有證書（即須續期的證書）到期日之後二年	新的數碼證書的有效期可超過二年，但不會超過二年另一個月
三年	新證書產生日期	原有證書（即須續期的證書）到期日之後三年	新的數碼證書的有效期可超過三年，但不會超過三年另一個月

附註：1. 參閱第 1.2.4 條

3.2.2.2　數碼證書（機構）或數碼證書（保密）不會自動續期。然而，若續期申請是透過數碼證書登記人平台提交，並由授權代表使用「智方便+」進行數碼簽署（如第 3.1.8.1(a) 節所指明），或使用第 3.1.8.1(c) 節所指明的有效數碼簽署，則可在授權代表毋須親身到場的情況下續期。在所有其他情況下，授權代表須向香港數碼證書頒發中心提交已正式填妥並簽署的證書續期申請表，以申請續期。續期申請程序的詳情載於香港數碼證書頒發中心網站。若授權代表已被更換，新授權代表須依照第 3.1.8.1(a) 或 (b) 節的規定完成並提交新的申請。

3.2.2.3　續期以後，只要登記人協議原有之條款及條件與續期當日有效之核證作業準則條款並無抵觸，則原訂的條文仍適用於新續期的證書。如兩者有所抵觸，則以續期當日之核證作業準則內的條款為準。申請人應細閱續期當日有效的核證作業準則，方可遞交續期申請表。

4． 運作要求

4.1 數碼證書（個人）

4.1.1 證書申請

4.1.1.1 處理申請

4.1.1.1.1　申請人必須透過數碼證書登記人平台，或在適用情況下，透過承辦商或註冊機構遞交數碼證書申請（見**附錄 E**）。

4.1.1.1.2　對於數碼證書（個人），申請人必須在申請時同意使用 PKCS#12 格式檔案以發出數碼證書及私人密碼匙。若數碼證書申請是透過數碼證書登記人平台遞交，申請人亦必須同意透過該平台下載檔案或香港數碼證書頒發中心指定的其他安全電子方式。否則，該檔案將儲存於數碼證書檔案 USB，作為數碼證書儲存媒體。

4.1.1.1.3　對於支援 Adobe PDF 簽署的數碼證書（個人），申請人必須在申請時選擇一個符合 PKCS#11 標準的裝置，作為發出數碼證書及私人密碼匙的數碼證書儲存媒體。

4.1.1.1.4　香港數碼證書頒發中心對所有用於存儲私人密碼匙的儲存媒體的預備、啟動、使用、分派及終止使用均制定有內部程序及控制措施，並定期經獨立第三方審核。

4.1.1.1.5　數碼證書申請表一經遞交，申請人即批准香港數碼證書頒發中心向其他人士或在香港儲存庫公布其數碼證書，並接受香港數碼證書頒發中心將發給申請人的數碼證書。

4.1.1.2 核對身分

申請人必須按照第 3.1.9(a)、(b) 及 (c) 所述其中一個程序，提供有效的身份證明。完成身份核驗程序並獲得滿意結果後，香港數碼證書頒發中心將產生用於存取數碼證書（個人）（包括相關密碼匙）的密碼。此數碼證書密碼在日後使用數碼證書及私人密碼匙時必須輸入，以防止未經授權的存取。

4.1.2 發出數碼證書

4.1.2.1　透過數碼證書登記人平台發出數碼證書（個人）

4.1.2.1.1　在核對身分手續後，香港數碼證書頒發中心會在其處所內之穩當系統及環境下產生申請人之數碼證書（包括配對密碼匙），以保證私人密碼匙不受干擾。

4.1.2.1.2　私人密碼匙及數碼證書將儲存於 PKCS#12 格式檔案（「數碼證書檔案」）中，供申請人下載，或儲存於數碼證書檔案 USB，作為數碼證書儲存媒體。若選擇符合 PKCS#11 標準的裝置作為數碼證書儲存媒體，則私人密碼匙及數碼證書將直接發出至該符合 PKCS#11 標準的裝置（詳見第 4.1.2.2 條）。

4.1.2.1.3　每個數碼證書檔案將以相關密碼保護。用於取得密碼的安全電子連結將以電郵方式另行發送予申請人。日後任何使用數碼證書檔案內的數碼證書及私人密碼匙，均須輸入相關密碼，以防止未經授權的存取。

4.1.2.1.4　數碼證書檔案將暫時保留於數碼證書登記人平台，供申請人下載。

4.1.2.1.5　已接受並發出的數碼證書將刊登於儲存庫。

4.1.2.1.6　申請人必須登入數碼證書登記人平台，並將數碼證書檔案下載至本地系統儲存。當申請人完成下載數碼證書檔案及取得相關密碼後，兩者均會於數碼證書登記人平台中被永久刪除。

4.1.2.2　發出數碼證書（個人）並載入數碼證書儲存媒體內

4.1.2.2.1　完成身份核驗程序後，香港數碼證書頒發中心將在其指定場所內的可信系統及環境中，為相關申請人產生數碼證書（包括相關密碼匙），以確保私人密碼匙不會遭到竄改。

4.1.2.2.2　私人密碼匙及數碼證書將儲存於申請人所選擇的數碼證書儲存媒體中。

4.1.2.2.3　每個數碼證書儲存媒體將以相關密碼保護。用於取得密碼的安全電子連結將以電郵方式另行發送予申請人。日後任何使用數碼證書儲存媒體內的數碼證書及私人密碼匙，均須輸入相關密碼，以防止未經授權的存取。

4.1.2.2.4　數碼證書儲存媒體將以防竄改封套或其他形式的容器安全封裝，並以安全方式交付予申請人，包括安全的派遞服務，例如掛號郵件等。

4.1.2.2.5　已接受並發出的數碼證書將刊登於儲存庫。

4.1.2.3　私人密碼匙

4.1.2.3.1　若數碼證書及私人密碼匙遺失或損毀，香港數碼證書頒發中心將無法恢復。因此，申請人須負責妥善保存數碼證書檔案或數碼證書儲存媒體，作為其數碼證書及私人密碼匙的備份。

4.1.2.3.2　儲存於數碼證書登記人平台及香港數碼證書頒發中心系統內的所有私人密碼匙均以加密形式保存，並設有適當的安全控制措施，以防止未經授權的存取及洩露加密的私人密碼匙。當完成將數碼證書及私人密碼匙交付予申請人後，相關私人密碼匙將從數碼證書登記人平台及香港數碼證書頒發中心系統中刪除。

4.1.2.4　核實證書資料

申請人可透過瀏覽證書檔案或儲存庫核實證書上的資料。如發現證書資料有任何錯誤，申請人應立即通知香港數碼證書頒發中心。

4.1.3 公布數碼證書

根據《電子交易條例》的規定，香港數碼證書頒發中心會盡快在儲存庫公布已獲接受並已發出的

數碼證書（見第 2.5 條）。申請人可瀏覽證書檔案或經香港數碼證書頒發中心儲存庫核實證書資料。一旦發現任何不正確的證書資料，申請人應立即通知香港數碼證書頒發中心。

4.2 數碼證書（機構）

4.2.1 證書申請

4.2.1.1 處理申請

4.2.1.1.1 申請數碼證書（機構）者必須遞交數碼證書申請，包括任何補充申請表及香港數碼證書頒發中心要求的所有其他文件，並須透過數碼證書登記人平台，或在適用情況下，透過承辦商或註冊機構遞交（見**附錄 E**）。

4.2.1.1.2 對於數碼證書（機構），申請人必須在申請時同意使用 PKCS#12 格式檔案以發出數碼證書及私人密碼匙。若數碼證書申請是透過數碼證書登記人平台遞交，申請人亦必須同意透過該平台下載檔案或香港數碼證書頒發中心指定的其他安全電子方式。否則，該檔案將儲存於數碼證書檔案 USB，作為數碼證書儲存媒體。

4.2.1.1.3 對於支援 Adobe PDF 簽署的數碼證書（機構），申請人必須在申請時選擇一個符合 PKCS#11 標準的裝置，作為發出數碼證書及私人密碼匙的數碼證書儲存媒體。

4.2.1.1.4 香港數碼證書頒發中心已實施內部程序及控制措施，以管理任何密碼儲存媒體的準備、啟用、使用、分發及終止。這些程序及控制措施會定期由獨立第三方審核。

4.2.1.1.5 遞交數碼證書申請即表示申請人授權將數碼證書刊登於儲存庫或提供予其他人士，並接受該數碼證書發出予申請人。

4.2.1.2 身份核驗

用於核實登記人機構、授權代表及授權用戶身份的文件要求載於本 CPS 第 3.1.8 條。完成身份核驗程序並獲得滿意結果後，香港數碼證書頒發中心將產生用於存取數碼證書（機構）（包括相關密碼匙）的密碼，並分配予各授權用戶。此數碼證書密碼在日後使用數碼證書及私人密碼匙時必須輸入，以防止未經授權的存取。

4.2.2 發出證書

4.2.2.1 透過數碼證書登記人平台發出數碼證書（機構）

4.2.2.1.1 在核對身分手續後，香港數碼證書頒發中心會在其處所內之穩當系統及環境下產生申請人之數碼證書（包括配對密碼匙），以保證私人密碼匙不受干擾。

4.2.2.1.2 每位授權用戶的私人密碼匙及數碼證書將儲存於個別的 PKCS#12 格式檔案（「數碼證書檔案」）中，供授權代表下載，或儲存於數碼證書檔案 USB，作為數碼證書儲存媒體。若選擇符合 PKCS#11 標準的裝置作為數碼證書儲存媒體，則私人密碼匙及數碼證書將直接發出至該符合 PKCS#11 標準的裝置（詳見第 4.2.2.2 條）。

4.2.2.1.3　授權代表須負責將各數碼證書檔案分發予相關授權用戶。每個數碼證書檔案將以相關密碼保護，用於取得密碼的安全電子連結將以電郵方式另行發送予各授權用戶。日後任何使用數碼證書檔案內的數碼證書及私人密碼匙，均須輸入相關密碼，以防止未經授權的存取。

4.2.2.1.4　數碼證書檔案將暫時保留於登記人平台，供授權代表下載。

4.2.2.1.5　已接受並發出的數碼證書將刊登於儲存庫。

4.2.2.1.6　授權代表必須登入數碼證書登記人平台，並將數碼證書檔案下載至本地系統儲存。當授權代表完成下載數碼證書檔案，且相關授權用戶已取得相關密碼後，兩者均會於數碼證書登記人平台中被永久刪除。

4.2.2.2　發出數碼證書（機構）並載入數碼證書儲存媒體內

4.2.2.2.1　完成身份核驗程序後，香港數碼證書頒發中心將在其指定場所內的可信系統及環境中，為相關授權用戶產生數碼證書（包括相關密碼匙），以確保私人密碼匙不會遭到竄改。

4.2.2.2.2　私人密碼匙及數碼證書將儲存於授權代表所選擇的數碼證書儲存媒體中。

4.2.2.2.3　每個數碼證書儲存媒體將以相關密碼保護。用於提取密碼的安全電子連結將以電郵方式另行發送予相關授權用戶。日後任何使用數碼證書儲存媒體內的數碼證書及私人密碼匙，均須輸入相關密碼，以防止未經授權的存取。

4.2.2.2.4　數碼證書儲存媒體將以防竄改封套或其他形式的容器安全封裝，並以安全方式交付予申請人，包括安全的派遞服務，例如掛號郵件等。

4.2.2.2.5　已接受並發出的數碼證書將刊登於儲存庫。

4.2.2.3　私人密碼匙

4.2.2.3.1　若數碼證書及私人密碼匙遺失或損毀，香港數碼證書頒發中心將無法恢復。因此，申請人須負責妥善保存數碼證書檔案或數碼證書儲存媒體，作為其數碼證書及私人密碼匙的備份。

4.2.2.3.2　儲存於數碼證書登記人平台及香港數碼證書頒發中心系統內的所有私人密碼匙均以加密形式保存，並設有適當的安全控制措施，以防止未經授權的存取及洩露加密的私人密碼匙。當完成將數碼證書及私人密碼匙交付予申請人後，相關私人密碼匙將從數碼證書登記人平台及香港數碼證書頒發中心系統中刪除。

4.2.2.4　核實證書資料

申請人可透過瀏覽證書檔案或儲存庫核實證書上的資料。如發現證書資料有任何錯誤，申請人應立即通知香港數碼證書頒發中心。

4.2.3 公布數碼證書

根據《電子交易條例》的規定，香港數碼證書頒發中心會盡快在儲存庫公布已獲接受並已發出的數碼證書（見第 2.5 條）。申請人可瀏覽證書檔案或經香港數碼證書頒發中心儲存庫核實證書資料。一旦發現任何不正確的證書資料，申請人應立即通知香港數碼證書頒發中心。

4.3 數碼證書（保密）

4.3.1 證書申請

4.3.1.1　處理申請

4.3.1.1.1　申請數碼證書（保密）者必須遞交數碼證書申請，包括任何補充申請表及香港數碼證書頒發中心要求的所有其他文件，並須透過數碼證書登記人平台，或在適用情況下，透過承辦商或註冊機構遞交（見**附錄 E**）。

4.3.1.1.2　申請人必須在申請時同意使用 PKCS#12 格式檔案以發出數碼證書及私人密碼匙。若數碼證書申請是透過數碼證書登記人平台遞交，申請人亦必須同意透過該平台下載檔案或香港數碼證書頒發中心指定的其他安全電子方式。否則，該檔案將儲存於數碼證書檔案 USB，作為數碼證書儲存媒體。

4.3.1.1.3　香港數碼證書頒發中心已實施內部程序及控制措施，以管理任何密碼儲存媒體的準備、啟用、使用、分發及終止。這些程序及控制措施會定期由獨立第三方審核。

4.3.1.1.4　遞交數碼證書申請即表示申請人授權將數碼證書刊登於儲存庫或提供予其他人士，並接受該數碼證書發出予申請人。

4.3.1.2　身份核驗

用於核實登記人機構、授權代表及授權用戶身份的文件要求載於本 CPS 第 3.1.8 條。完成身份核驗程序並獲得滿意結果後，香港數碼證書頒發中心將產生用於存取數碼證書（保密）（包括相關密碼匙）的密碼，並分配予各授權單位。此數碼證書密碼在日後使用數碼證書及私人密碼匙時必須輸入，以防止未經授權的存取。

4.3.2 發出證書

4.3.2.1　透過數碼證書登記人平台發出數碼證書（保密）

4.3.2.1.1 在核對身分手續後，香港數碼證書頒發中心會在其處所內之穩當系統及環境下產生申請人之電子證
書（包括配對密碼匙），以保證私人密碼匙不受干擾。

4.3.2.1.2 每個授權單位的私人密碼匙及數碼證書將儲存於個別的 PKCS#12 格式檔案（「數碼證書

檔案」）中，供授權代表下載，或儲存於數碼證書檔案 USB，作為數碼證書儲存媒體（詳見第 4.3.2.2 條）。

4.3.2.1.3 授權代表須負責將各數碼證書檔案分發予相關授權單位。每個數碼證書檔案將以相關密碼保護，用於提取密碼的安全電子連結將以電郵方式另行發送予相關授權單位。日後任何使用數碼證書檔案內的數碼證書及私人密碼匙，均須輸入相關密碼，以防止未經授權的存取。

4.3.2.1.4 數碼證書檔案將暫時保留於登記人平台，供授權代表下載。

4.3.2.1.5 已接受並發出的數碼證書將刊登於儲存庫。

4.3.2.1.6 授權代表必須登入數碼證書登記人平台，並將數碼證書檔案下載至本地系統儲存。當授權代表完成下載數碼證書檔案，且相關授權單位已提取相關密碼後，相關私人密碼匙將從數碼證書登記人平台及香港數碼證書頒發中心系統中刪除。

4.3.2.2　發出數碼證書（保密）並載入數碼證書儲存媒體內

4.3.2.2.1 在核對身分手續後，香港數碼證書頒發中心會在其處所內之穩當系統及環境下產生申請人之電子證
書（包括配對密碼匙），以保證私人密碼匙不受干擾。

4.3.2.2.2 私人密碼匙及數碼證書將儲存於授權代表所選擇的數碼證書儲存媒體中。

4.3.2.2.3 每個數碼證書儲存媒體將以相關密碼保護。用於提取密碼的安全電子連結將以電郵方式另行發送予相關授權單位。日後任何使用數碼證書儲存媒體內的數碼證書及私人密碼匙，均須輸入相關密碼，以防止未經授權的存取。

4.3.2.2.4 數碼證書儲存媒體將以防竄改封套或其他形式的容器安全封裝，並以安全方式交付予申請人，包括安全的派遞服務，例如掛號郵件等。

4.3.2.2.5 已接受並發出的數碼證書將刊登於儲存庫。

4.3.2.3　私人密碼匙

4.3.2.3.1 若數碼證書及私人密碼匙遺失或損毀，香港數碼證書頒發中心將無法恢復。因此，申請人須負責妥善保存數碼證書檔案或數碼證書儲存媒體，作為其數碼證書及私人密碼匙的備份。

4.3.2.3.2 儲存於數碼證書登記人平台及香港數碼證書頒發中心系統內的所有私人密碼匙均以加密形式保存，並設有適當的安全控制措施，以防止未經授權的存取及洩露加密的私人密碼匙。當完成將數碼證書及私人密碼匙交付予申請人後，相關私人密碼匙將從數碼證書登記人平台及香港數碼證書頒發中心系統中刪除。

4.3.2.4　核實證書資料

申請人可透過瀏覽證書檔案或儲存庫核對證書上的資料。如發現證書資料有任何錯誤，申請人應立即通知香港數碼證書頒發中心。

4.3.3 公布數碼證書

根據《電子交易條例》的規定，香港數碼證書頒發中心會盡快在儲存庫公布已獲接受並已發出的數碼證書（見第 2.5 條）。申請人可瀏覽證書檔案或經香港數碼證書頒發中心儲存庫核實證書資料。一旦發現任何不正確的證書資料，申請人應立即通知香港數碼證書頒發中心。

4.4 證書申請的處理期限

香港數碼證書頒發中心將作出合理努力，確保在合理的時間內完成證書申請。在登記人提交的證書申請資料齊全並且符合要求的情況下，香港數碼證書頒發中心承諾完成證書申請時間如下：

證書類別	完成證書申請時間
數碼證書（個人）	三個工作天
數碼證書（機構）	十個工作天
數碼證書（保密）	

特此聲明，星期六、星期日、公眾假期及懸掛八號或以上之熱帶氣旋警告信號或黑色暴雨警告信號之工作日，就此 4.4 條而言，一律不視作工作日計算。

4.5 暫時吊銷及撤銷證書

4.5.1 暫時吊銷及撤銷

4.5.1.1 若香港數碼證書頒發中心私人密碼匙資料外洩，會導致香港數碼證書頒發中心迅速地撤銷所有經由該私人密碼匙發出的證書。在私人密碼匙資料外洩的情況下，香港數碼證書頒發中心會根據在密碼匙資料外洩計劃內定明的程序迅速地撤銷所有已發出的登記人證書（見第 4.10.2 條）。

4.5.1.2 按照準則中列明之撤銷程序，各登記人可於任何時間以任何理由要求撤銷依據本登記人協議須由其承擔責任之證書。

4.5.1.3 登記人之私人密碼匙或內載與某數碼證書公開密碼匙相關私人密碼匙之儲存媒體，若已外洩或懷疑已外洩，或數碼證書上由登記人提供之資料有任何改變，各登記人必須立即按照本準則的撤銷程序，向香港數碼證書頒發中心申請撤銷證書（見第 2.1.4(k) 條）。

4.5.1.4 不論何時，若有以下情況，香港數碼證書頒發中心均可按準則中程序暫時吊銷或撤銷證書並會以電子郵件（證書撤銷通知書（如有電子郵件地址））及透過更新證書撤銷清單的方式通知登記人：

a) 知道或有理由懷疑登記人之私人密碼匙已外洩；
b) 知道或有理由懷疑證書之細節不真實或已變得不真實或證書不可靠；

c) 認為證書並非根據準則妥當發出；
d) 認為登記人未有履行本準則或登記人協議列明之責任；
e) 證書適用之規例或法例有此規定；
f) 認為登記人未曾繳付登記費；
g) 知道或有理由相信其資料出現在數碼證書（個人）上之登記人：
   i) 死亡或已死亡；
   ii) 在擬撤銷證書前五年內已達成香港法例第六章破產條例所指之債務重整協議或債務償還安排或自願安排；或
   iii) 因欺詐、舞弊或不誠實行為，或違反電子交易條例而在本港或其他地方被定罪；

h) 知道或有理由相信在數碼證書（機構）上指明之授權用戶已非登記人機構之成員或僱員；
i) 知道或有理由相信其資料出現在數碼證書（機構）或數碼證書（保密）上之登記人：
   (i) 正被清盤或接到有司法管轄權之法庭所判清盤令；
   (ii) 在擬撤銷證書前五年內已達成香港法例第六章破產條例所指之債務重整協議或債務償還安排或自願安排；
   (iii) 其董事、職員或僱員因欺詐、舞弊或不誠實行為，或違反電子交易條例被定罪；
   (iv) 在撤銷證書前五年內登記人資產之任何部分託給接管人或管理人接管；或
   (v) 無法證明登記人之存在。

4.5.1.5 香港數碼證書頒發中心將嚴格控制，作出合理努力避免由於證書製作過程中的失誤（例如證書下載錯誤、密碼匙不匹配）而導致證書吊銷。

4.5.2 撤銷程序請求

登記人，或登記人機構的授權代表，可透過香港數碼證書頒發中心網站的指定網頁、數碼證書登記人平台、電郵或親身遞交方式，向香港數碼證書頒發中心遞交撤銷證書申請。

香港數碼證書頒發中心在收到撤銷申請後，會核實該申請並確認撤銷的原因，然後暫停相關證書。當 香港數碼證書頒發中心 收到由登記人或最初接收撤銷申請的註冊機構所發出的最終撤銷確認後，該證書將被撤銷，其有效性將被永久終止。最終撤銷確認可包括以下其中之一：於數碼證書登記人平台上的確認訊息、由登記人以其私人密碼匙進行數碼簽署的電郵、由登記人親筆簽署的原件信函，或由登記人簽署的撤銷證書申請表。撤銷證書申請表可於 香港數碼證書頒發中心 網站取得。
如未有收到登記人的最後確認，證書會繼續暫時失效，並列入證書撤銷清單，直至證書有效期屆滿為止。香港數碼證書頒發中心 會考慮登記人的要求，把暫時吊銷的證書恢復為有效。但 香港數碼證書頒發中心 只會在謹慎的情況下把暫時吊銷的證書恢復為有效。

所有被暫時吊銷或撤銷證書之有關資料（包括表明暫時吊銷或撤銷證書的原因代碼）會刊載於證書撤銷清單（見第 7.2 條）。下次更新的證書撤銷清單不會包括由「暫時吊銷」狀態恢復有效的證書。

香港數碼證書頒發中心 處理以電郵或親身遞交之撤銷申請的辦公時間如下：

星期一至星期五	: 上午 9 時至下午 5 時
星期六、星期日及公眾假期	: 暫停服務

如懸掛八號或以上之熱帶氣旋警告信號或黑色暴雨警告信號，將立即暫停處理撤銷證書申請。處理將按下列情況恢復：

- 如在該日早上六時或以前除下信號，處理將於當日的正常辦公時間恢復。
- 如信號在早上六時後至上午十時或以前除下，處理將於當日下午二時（星期六、星期日及公眾假期除外）恢復。
- 如信號在上午十時後除下，處理將於下一個工作日的正常辦公時間（星期六、星期日及公眾假期除外）恢復。

4.5.3 服務承諾、證書撤銷清單的更新

a) 香港數碼證書頒發中心將作出合理合理努力，確保在 (1) 香港數碼證書頒發中心從登記人處收到撤銷證書申請或撤銷證書的最後確認或 (2) 在無此申請之情況下，香港數碼證書頒發中心決定暫時吊銷或撤銷證書，兩個工作日內，將該暫時吊銷或撤銷證書資料於證書撤銷清單公布。

然而，證書撤銷清單並不會於各證書暫時吊銷或撤銷後隨即在公眾目錄中公布。祇有在下一份證書撤銷清單更新時一併公布，證書撤銷清單介時才會顯示該證書已暫時吊銷或撤銷之狀態。證書撤銷清單每日公布，並存檔最少七年。

特此聲明，星期六、星期日、公眾假期及懸掛八號或以上之熱帶氣旋警告信號或黑色暴雨警告信號之工作日，就此 4.5.3（a）條而言，一律不視作工作日計算。

香港數碼證書頒發中心會以合理的方式，盡量在收到撤銷證書申請兩個工作天內，透過電子郵件（如有電子郵件地址）及更新證書撤銷清單的方式向有關登記人發出撤銷證書通知。

b) 在登記人明知香港數碼證書頒發中心根據準則條款可能據以撤銷證書之任何事項之情況下，或登記人已作出撤銷申請或經知會香港數碼證書頒發中心，香港數碼證書頒發中心擬根據本準則條款暫時吊銷或撤銷證書後，登記人均不得在交易中使用證書。倘若登記人無視本條所述的規定，仍確實在交易中使用證書，則香港數碼證書頒發中心毋須就任何該等交易向登記人或倚據人士承擔責任。

c) 此外，登記人明知香港數碼證書頒發中心根據準則可能據以撤銷證書之任何事項之情況下撤銷證書，或登記人作出申請或經知會香港數碼證書頒發中心擬撤銷證書時，須立即通知從事當時仍有待完成之任何交易之倚據人士，用於該交易之證書須予撤銷 (由香港數碼證書頒發中心或經登記人申請)，並明確說明，因情況乃屬如此，故倚據人士不得就交易而倚據證書。若登記人未能通知倚據人士，則香港數碼證書頒發中心無須就該等交易向登記人承擔責任，並無須向雖已收到通知但仍完成交易之倚據人士承擔責任。

除非香港數碼證書頒發中心未能行使合理技術及謹慎且登記人未能按此等規定之要求通知倚據人士，否則，香港數碼證書頒發中心無須就香港數碼證書頒發中心作出暫時吊銷或撤銷證書(根據申請或其他原因)之決定與此資訊出現於證書撤銷清單之間，或者就作出暫時吊銷或撤銷證書之決定之時間內進行之交易承擔責任。任何此等責任均僅限於本準則其他部分規限之範疇。在任何情況下，核證登記機關自身無須對倚據人士承擔獨立謹慎責任（核證登記機關只是履行香港數碼證書頒發中心之謹慎責任）。因此，即使出現疏忽，核證登記機關亦無須對倚據人士負責。

d) 當電子認證服務機構本身的證書被暫時吊銷或撤銷時，香港數碼證書頒發中心將及時發佈有關信息(包括證書撤銷清單（如香港數碼證書頒發中心授權撤銷清單 ARL）。

e) 證書撤銷清單、香港數碼證書頒發中心授權撤銷清單 ARL 會依據在**附錄 C** 內指明的時間表及格式更新及公布。補充證書撤銷清單會在特殊的情況下於香港數碼證書頒發中心網頁公布。

f) 有關香港數碼證書頒發中心對於倚據人士暫時未能獲取已暫時吊銷或撤銷的證書資料時的政策，已列於本準則第 2.1.6 條(倚據人士之義務)及 2.2.1 條(合理技術及謹慎)。

4.5.4 撤銷效力

在香港數碼證書頒發中心把暫時吊銷 / 撤銷狀況刊登到證書撤銷清單，即終止某一證書。

4.6 證書登記使用期的結束

以下三種情況將被視為證書登記使用期結束

a) 在證書有效期內，證書被香港數碼證書頒發中心撤銷；
b) 在證書到期前提出終止服務的申請，並獲香港數碼證書頒發中心接受；
c) 證書有效期滿，沒有進行證書更新或密碼匙更新。

香港數碼證書頒發中心已備有明確關於證書訂購結束的規定，指導證書訂購結束的具體實施流程，並妥善保存記錄至第 4.8.2 條指定之最短之時限。

4.7 電腦保安審核程序

4.7.1 記錄事件類型

香港數碼證書頒發中心核證機關系統內之重要保安事件，均以人手或自動記錄在受保護的審核追踪檔案內。此等事件包括而不限於以下例子：

- 可疑網絡活動
- 多次試圖進入而未能接達
- 與安裝設備或軟件、修改及配置核證機關運作之有關事件
- 享有特權接達核證機關各組成部分的過程
- 定期管理證書之工作包括：
    - 處理撤銷及暫時吊銷證書之要求
    - 實際發出、撤銷及暫時吊銷證書
    - 證書續期
    - 更新儲存庫資料
    - 匯編撤銷證書清單並刊登新資料
    - 核證機關密碼匙轉換
    - 檔案備存
    - 緊急密碼匙復原

4.7.2 處理紀錄之次數

香港數碼證書頒發中心每日均會處理及覆檢審核運行紀錄，用以審核追蹤有關香港數碼證書頒發中心核證機關的行動、交易及程序。

4.7.3 審核紀錄之存留期間
存檔審核紀錄文檔存留期為七年。

4.7.4 審核紀錄之保護
香港數碼證書頒發中心處理審核紀錄時實施多人式控制，可提供足夠保護，避免有關紀錄意外受損或被人蓄意修改。

4.7.5 審核紀錄備存程序
香港數碼證書頒發中心每日均會按照預先界定程序(包括多人式控制)為審核紀錄作適當備存。備存會另行離機儲存，並獲足夠保護，以免被盜用、損毀及媒體衰變。備存入檔前會保留至少一星期。

4.7.6 審核資料收集系統
香港數碼證書頒發中心核證機關系統審核紀錄及文檔受自動審核收集系統控制，該收集系統不能為任何應用程式、程序或其他系統程式修改。任何對審核收集系統之修改本身即成為可審核事件。

4.7.7 事件主體向香港數碼證書頒發中心發出通知
香港數碼證書頒發中心擁有自動處理系統，可向適當人士或系統報告重要審核事件。

4.7.8 脆弱性評估
脆弱性評估為香港數碼證書頒發中心核證機關保安程序之一部份。

4.8 紀錄存檔

4.8.1 存檔紀錄類型
香港數碼證書頒發中心須確保存檔紀錄記下足夠資料，可確定證書是否有效以及以往是否運作妥當。香港數碼證書頒發中心(或由其代表)存有以下數據：

- 系統設備結構檔案
- 評估結果及/或設備合格覆檢(如曾進行)
- 核證作業準則及其修訂本或最新版本
- 對香港數碼證書頒發中心具約束力而構成合約之協議
- 所有發出或公布之證書及證書撤銷清單
- 定期事件紀錄
- 其他需用以核實存檔內容之數據
- 證書系統建設和升級文檔；
- 證書申請支持文檔，證書服務批准和拒絕的信息，與證書訂戶的協議；
- 審計記錄；
- 員工資料，包括但不限於背景調查、錄用、培訓等資料；
- 各類外部、內部評估文檔。

4.8.2 存檔保存期限
密碼匙及證書資料以及 4.8.1 中提及之存檔須妥為保存最少七年。審核跟蹤文檔須以香港數碼證書頒發中心視為適當之方式存放於系統內。

4.8.3 存檔保護
香港數碼證書頒發中心保存之存檔媒體受各種實體或加密措施保護，可避免未經授權進入。保

護措施用以保護存檔媒體免受溫度、濕度及磁場等環境侵害。

4.8.4 存檔備份程序

在有需要時製作並保存存檔之副本。歸檔時，須對歸檔記錄的一致性進行驗證。歸檔期間，須通過適當的技術或方法驗證所有被訪問的記錄的一致性。

4.8.5 電子郵戳

存檔資料均註明開設存檔項目之時間及日期。香港數碼證書頒發中心利用控制措施防止擅自調校自動系統時鐘。

4.9 密碼匙變更

由香港數碼證書頒發中心產生，並用以證明根據本準則發出的證書的核證機關根源密碼匙及證書有效期為不超過二十五年（見**附錄 G**）。香港數碼證書頒發中心核證機關密碼匙及證書在期滿前至少三個月會進行續期。續發新根源密碼匙後，相應之根源證書會在香港數碼證書頒發中心網頁公布供大眾取用。原先之根源密碼匙則保留至第 4.8.2 條指定之最短之時限，以供核對用原先密碼匙進行產生之簽署。確保整個過渡過程安全、順利，並力求減少對登記人和倚據人士的影響。

4.10 災難復原及密碼匙資料外洩之應變計劃

4.10.1 災難復原計劃

香港數碼證書頒發中心已備有妥善管理之程序，包括每天為主要業務資訊及核證系統的資料備存及適當地備存核證系統的軟件，以維持主要業務持續運作，保障在嚴重故障或災難影響下仍可繼續業務。業務持續運作計劃之目的在於促使香港數碼證書頒發中心核證機關全面恢復提供服務，內容包括一個經測試的獨立災難復原基地，而該基地現時位於香港特別行政區內並距離核證機關主要營運設施不少於十千米。業務持續運作計劃每年均會檢討及進行演練，而有關主要人員均須參與，並對演練程序和結果進行記錄。

如發生嚴重故障或災難，香港數碼證書頒發中心會即時知會數字政策專員，並公布運作由生產基地轉至災難復原基地。

在發生災難後但穩妥可靠的環境尚未重新確立前：

a) 敏感性物料或儀器會安全地鎖於設施內；
b) 若不能將敏感性物料或儀器安全地鎖於設施內或該等物料或儀器有受損毀的風險，該等物料或儀器會移離設施並鎖於其他臨時設施內；及
c) 設施的出入通道會實施接達管制，以防範盜竊及被人擅自接達。

4.10.2 密碼匙資料外洩之應變計劃

業務持續運作計劃內載處理密碼匙資料外洩之正式程序。此等有關程序每年均會檢討及執行。

如根據本準則發出數碼證書的香港數碼證書頒發中心私人密碼匙資料外洩，香港數碼證書頒發中心會即時知會數字政策專員並作出公布。香港數碼證書頒發中心的私人密碼匙資料一旦外洩，香港數碼證書頒發中心會即時撤銷根據有關私人密碼匙發出之證書，然後發出新證書取代，並且在合理的時間內採用適當的方式及時通知登記人和倚據人士。

4.10.3 密碼匙的替補

倘若在密碼匙資料外洩或災難情況下，香港數碼證書頒發中心根據本準則發出數碼證書的私人

密碼匙資料外洩或遭破壞而無法復原，香港數碼證書頒發中心會儘快知會數字政策專員並作出公布。公布內容包括已撤銷證書的名單、如何為登記人提供新的香港數碼證書頒發中心公開密碼匙及如何向登記人重新發出證書。香港數碼證書頒發中心核證機關根源證書的撤銷請求，必須經過數字政策專員確定後才可以進行。

4.10.4 計算機資源、軟件和/或數據的損壞

業務持續運作計劃內包含計算資源、軟件和/或數據的損壞之正式程序。此等有關程序每年均會檢討及進行演練。

當發生計算機資源、軟件和/或數據的損壞，香港數碼證書頒發中心將評估事件的影響，調查原因，根據系統內部備份的資料，執行系統恢復操作，使認證系統能夠重新正常運行。倘若在計算機資源、軟件和/或數據損壞的情況下，香港數碼證書頒發中心根據本準則發出數碼證書的私人密碼匙資料外洩或遭破壞而無法復原，香港數碼證書頒發中心會儘快知會數字政策專員並作出公布。倘若在計算機資源、軟件和/或數據損壞的情況下，香港數碼證書頒發中心為登記人代製的私人密碼匙資料外洩或遭破壞而無法復原，香港數碼證書頒發中心會即時撤銷有關證書，然後發出新證書取代，並且在合理的時間內採用適當的方式及時通知登記人和倚據人士。

4.11 核證機關終止服務

如香港數碼證書頒發中心停止擔任核證機關之職能，即按“香港數碼證書頒發中心終止服務計劃”所定程序知會數字政策專員並作出公布。在終止服務後，香港數碼證書頒發中心會將核證機關的紀錄適當地存檔七年（由終止服務日起計）；該等紀錄包括已發出的證書、根源證書、核證作業準則及證書撤銷清單。

4.12 核證登記機關終止服務

如核證登記機關根據核證登記機關協議或因核證機關終止服務（第 4.11 條）停止擔任核證登記機關之職能，或其代表香港數碼證書頒發中心行使之授權已予以收回，經由該核證登記機關申請之證書仍會按其條款及有效期繼續有效。

5． 實體、程序及人員保安控制

5.1 實體保安

5.1.1 選址及建造

香港數碼證書頒發中心核證機關運作位於商業上具備合理實體保安條件之地點。在場地建造過程中，香港數碼證書頒發中心已採取適當預防措施，為核證機關運作作好準備。

5.1.2 進入控制

5.1.2.1 數據中心

香港數碼證書頒發中心採取措施保護其設備免遭未經授權的存取，並實施實體控制，以減低設備被篡改的風險。香港數碼證書頒發中心系統所運行的數據中心由保安人員全年 365 日，每日 24 小時當值。存取設置認證平台的數據中心必須使用雙重認證——個人必須同時持有獲授權的存取卡並通過生物認證存取控制系統。這些生物認證存取系統會記錄每一次使用存取卡的情況。

5.1.2.2 核證登記機關運作區域

香港數碼證書頒發中心已實施商業上合理的實體保安控制，以劃分不同的保安區域，並根據各區域的要求採取有效的實體保安措施，以確保相關區域的實體安全。同時，香港數碼證書頒發中心會確保存取各個實體保安層均可被審計及受控，使只有獲授權人員方可存取每一個實體保安層。

5.1.3 機房環境控制

香港數碼證書頒發中心的數據中心無間斷有人員當值。然而，如香港數碼證書頒發中心知悉某個數據中心即將長時間無人當值，或已經長時間無人當值，香港數碼證書頒發中心人員將對該數據中心進行安全檢查，以確認：

a) 香港數碼證書頒發中心的設備處於符合當前運作模式的狀態，
b) 所有安全儲存設施均已妥善上鎖，
c) 實體安全系統（例如電腦機櫃鎖）運作正常，及
d) 該區域已妥善防止未經授權的進入。

監察系統會對基礎設施設備、電腦機櫃及安全防護系統進行實體安全監察，服務時間為每日 24 小時、每週 7 天。監察記錄將保留 3 個月，以用於故障診斷及事後審計。

5.1.4 電力及空調

核證機關設施可獲得之電力和空調資源包括專用的空調系統，無中斷電力供應系統及一台獨立後備發電機，以備城市電力系統發生故障時供應電力。

5.1.5 自然災害

核證機關設施在合理可能限度內受到保護，以免受自然災害影響。

5.1.6 防火及防水處理

數據中心配備滅火裝置，包括已安裝的消防設備，以及煙霧及溫度感應器。所有防火措施均符合香港消防處的要求。火警報警系統與滅火系統已連接運作。安置香港數碼證書頒發中心系統的機櫃設於高架地板之上，數據中心亦設有監察系統，以偵測水浸及漏水情況。

5.1.7 媒體存儲
媒體存儲及處置程序已經開發備妥。

5.1.8 場外備存
香港數碼證書頒發中心已建立關鍵系統（包括香港數碼證書頒發中心核證系統）和數據（包括審計數據在內的任何敏感信息）的備份制度及作場外儲存，並獲足夠保護，以免被盜用、損毀及媒體衰變。（另見第 4.10.1 條）

5.1.9 登記人協議及其他文件的保管
以電子方式遞交的登記人協議及身分確認文件將由香港數碼證書頒發中心、其承辦商或其核證登記機關，按照適用的資料保障及安全政策予以安全保存。只有獲授權人員方可查閱該等記錄，並已採取適當的保安措施，以防止未經授權的查閱或披露。

5.1.10 廢物處理
香港數碼證書頒發中心將謹慎處理包含隱私或者敏感信息的任何廢棄物，保證對此類廢棄物進行徹底的物理銷毀或信息刪除，避免這類廢物中包含的隱私或敏感信息被非授權使用、訪問或披露。

5.2 程序控制

5.2.1 受信職責
可進入或控制密碼技術或其他運作程序並可能會對證書之發出、使用或撤銷帶來重大影響（包括進入香港數碼證書頒發中心核證機關資料庫之受限制運作）之香港數碼證書頒發中心、承辦商或代表香港數碼證書頒發中心之核證登記機關僱員、承包商及顧問（統稱“人員”），應視作承擔受信職責。該等人員包括但不限於系統管理人員、操作員、工程人員及獲委派監督香港數碼證書頒發中心核證機關運作之行政人員。根據工作性質和職位權限的情況，賦予在承擔受信職責之人員在系統和物理環境中的權限，採用合適的訪問控制技術，以完整地記錄該人員所有敏感的操作行為。

香港數碼證書頒發中心已為所有涉及香港數碼證書頒發中心數碼證書服務而承擔受信職責之人員訂立、匯編及推行相關程序。執行下列工作，有關程序即可完整進行：

- 按角色及責任訂定各級實體及系統接達控制
- 採取職責分離措施

5.2.2 香港數碼證書頒發中心、承辦商與核證登記機關之間的文件及資料傳遞
香港數碼證書頒發中心、承辦商與核證登記機關之間的所有文件及資料的傳遞，均使用香港數碼證書頒發中心所慣常規定在控制及安全的方式進行。

5.2.3 年度評估
評估工作每年執行一次，以確保符合政策及工作程序控制之規定。（見第 2.6 條）

5.3 人員控制

5.3.1 背景及資格
香港數碼證書頒發中心及承辦商採用之人員及管理政策可合理確保香港數碼證書頒發中心、承辦商或代表香港數碼證書頒發中心之核證登記機關的人員，包括僱員、承包商及顧問之可信程

度及勝任程度，並確保他們以符合本準則之方式履行職責及表現令人滿意。

5.3.2 背景調查

香港數碼證書頒發中心對擔任受信職責之人員進行當面調查（其受聘前及其後有需要時定期進行並要求被調查人提供有效身份證件），及/或香港數碼證書頒發中心要求承辦商及核證登記機關進行調查，以根據本準則及香港數碼證書頒發中心之人員政策要求核實僱員之可信程度及勝任程度。未能通過首次及定期調查之人員不得擔任或繼續擔任受信職責。此外，在員工合同內已加入與安全相關的條款，在有關的人員在受聘前必須同意並簽署。

5.3.3 培訓要求

香港數碼證書頒發中心及承辦商及核證登記機關確保其所有人員（包括充當可信角色的人員）具備所需的技術資格和專業知識，以便能夠有效地履行職責，同時須為其員工提供適當及足夠的培訓（核心崗位至少每年一次），以確保他們執行任務的能力和安全策略得以有效的推行和遵守。綜合培訓內容包括但不限於：

a) 適當的技術培訓；
b) 規章制度和程序；
c) 處理安全事故及通知高層管理人員有關重大安全事故的程序。

5.3.4 在職人員的工作考察

香港數碼證書頒發中心及承辦商及核證登記機關確保制定適當的控制措施以考察人員的表現，例如：

a) 定期進行的工作績效考核；
b) 正規的紀律程序（其中包括如何處置未獲授權的行為）；
c) 正規的終止服務程序。

5.3.5 向人員提供之文件

香港數碼證書頒發中心及承辦商及核證登記機關人員會收到綜合用戶手冊，詳細載明證書之製造、發出、更新、續期及撤銷程序及與其職責有關之其他軟件功能。

6． 技術保安控制

本條說明香港數碼證書頒發中心特別為保障加密密碼匙及相關數據所訂之技術措施。控制香港數碼證書頒發中心核證機關密碼匙之工作透過實體保安及穩妥密碼匙存儲進行。產生、儲存、使用及毀滅香港數碼證書頒發中心核證機關密碼匙只能在由多人式控制之可防止篡改硬件裝置內進行。

6.1 密碼匙之產生及安裝

6.1.1 產生配對密碼匙

除非程序被獲授權使用者外洩，否則香港數碼證書頒發中心及申請人/登記人配對密碼匙之產生程序可使配對密碼匙的獲授權使用者以外人士無法取得私人密碼匙。香港數碼證書頒發中心產生配對根源密碼匙，用以發出符合本準則之證書。倘若由香港數碼證書頒發中心為申請人代製密碼匙，在完成送遞數碼證書及私人密碼匙給申請人後，申請人的私人密碼匙會從香港數碼證書頒發中心系統中刪除。

6.1.2 登記人公開密碼匙交付

香港數碼證書頒發中心會代表申請人 / 登記人按照代製密碼匙的要求產生數碼證書（個人）、數碼證書（機構）及數碼證書（保密）的配對密碼匙。

6.1.3 公開密碼匙交付予登記人

用於核證機關數碼簽署之各香港數碼證書頒發中心配對密碼匙之公開密碼匙可從網頁 https://www.hkca.hk 取得。香港數碼證書頒發中心採取保護措施，以防該等密碼匙被人更改。

6.1.4 密碼匙大小

香港數碼證書頒發中心於其根認證機關證書、下屬認證機關證書及登記人證書中使用下列 RSA 密碼匙長度及雜湊演算法。所有類型的證書均必須符合下文所列出的演算法及密碼匙長度要求。

證書類型	雜湊演算法	最小 RSA 模數長度（位元）
根源證書	SHA-256	4096
中繼證書	SHA-256	2048
登記人證書	SHA-256	2048

6.1.5 加密模組標準

香港數碼證書頒發中心進行之產生簽署密碼匙、存儲及簽署操作在硬件加密模組進行。

6.1.6 密碼匙用途

香港數碼證書頒發中心數碼證書(個人)、數碼證書（機構）及數碼證書（保密）之密碼匙可用於數碼簽署以及加密電子通訊。香港數碼證書頒發中心根源密碼匙（用於製造或發出符合本準則證書之密碼匙）只用於數碼簽署如簽署(a）及(b）撤銷清單。

6.2 私人密碼匙保護

6.2.1 加密模組標準

香港數碼證書頒發中心私人密碼匙利用加密模組產生，其級別至少達到 FIPS 140-2 第 3 級。

6.2.2 私人密碼匙多人式控制

香港數碼證書頒發中心私人密碼匙儲存在可防止篡改加密硬件裝置內。香港數碼證書頒發中心採用多人式控制（3 選 2 多人控制）啟動、使用、終止香港數碼證書頒發中心私人密碼匙。

6.2.3 私人密碼匙托管

香港數碼證書頒發中心使用之數碼證書系統並無為香港數碼證書頒發中心私人密碼匙及登記人私人密碼匙設計私人密碼匙托管程序。有關香港數碼證書頒發中心私人密碼匙的備存，見第 6.2.4 條。

6.2.4 香港數碼證書頒發中心私人密碼匙備存

香港數碼證書頒發中心私人密碼匙的備存，是使用達到 FIPS 140-2 第 3 級保安標準的裝置加密及儲存。香港數碼證書頒發中心私人密碼匙的備存程序須經超過一名人士參與完成。備存的私人密碼匙亦須超過一名人士啟動。其他私人密碼匙均不設備存。所有私人密碼匙不會存檔。

6.2.5 私人密碼匙於密碼模組之間傳遞

當香港數碼證書頒發中心私人密碼匙從一個硬件加密模組傳遞到另一個硬件加密模組上時，該私人密碼匙會以加密的形式在模組之間傳遞，並且在傳遞前要進行模組間的相互身份鑒別。另外香港數碼證書頒發中心還有嚴格的管理流程對私人密碼匙的傳遞進行控制，以確保有效防止了私人密碼匙的丟失、被竊、修改、非授權的使用或洩露。

6.3 配對密碼匙管理其他範疇

香港數碼證書頒發中心核證機關根源密碼匙使用期不超過由香港數碼證書頒發中心產生之簽署根源密碼匙及證書的有效期（見**附錄 G** 及第 4.9 條）。所有香港數碼證書頒發中心密碼匙之產生、銷毀、儲存以及證書、撤銷清單簽署運作程序，均於硬件加密模組內進行。第 4.8 條詳述香港數碼證書頒發中心公開密碼匙紀錄存檔之工作。

6.4 電腦保安控制

香港數碼證書頒發中心實行多人控制措施，控制啟動數據（如個人辨識密碼及接達核證機關系統密碼的生命周期）。香港數碼證書頒發中心已制定保安程序，防止及偵測未獲授權進入核證機關系統、更改系統及系統資料外洩等情況，確保電子認證服務機構軟件和存儲數據文件的系統是安全、可信賴的系統，不會受到未經授權的內部和外部訪問。此等保安控制措施接受第 2.6 條遵守規定之評估。香港數碼證書頒發中心實行嚴格的管理體系來控制和監視運行系統，以防止未授權的修改。在處理廢舊設備時，香港數碼證書頒發中心將盡合理努力，刪除所有可能影響認證業務安全性的信息存儲並加以確認。

6.5 生命週期技術保安控制

香港數碼證書頒發中心制定控制程序，為香港數碼證書頒發中心核證機關系統購置及發展軟件及硬件。並已定下更改控制程序以控制並監察就有關系統部件所作的調整及改善。
這些程序及措施的內容包括但不限於：

a) 無論由電子認證服務機構人員或在特殊情況下由其它機構進行開發工作，均能使用一致和有效的內部標準；
b) 將生產及開發的環境分隔開的有效程序；
c) 將操作、運維、開發人員的職責得以區分的有效程序；
d) 對用於生產及開發的環境內的資料及系統進行有效訪問的控制措施；

e) 對變更控制程序（包括但不限於系統和數據的正常和緊急變更）的有效控制措施（包括但不限於版本的控制、嚴格的測試驗證等）；
f) 系統上線前進行安全性的檢查和評估的程序，檢查和評估內容包括有否安全漏洞和被入侵的危險等；
g) 對採購設備及服務進行妥善管理的有效程序；
h) 硬件密碼匙設備的生命週期（從設備開始運作到邏輯/物理銷毀）過程中，對該設備的訪問至少有 3 名可信人員共同參與。

6.6 網絡保安控制

香港數碼證書頒發中心核證機關系統採用多級防火牆、入侵檢測、安全審計、病毒防範系統及其他接達控制機制來保護電子認證服務機構網絡環境的安全，適時更新版本，定期針對網絡環境進行風險評估和審計，以檢測有否被入侵的危險，其配置只允許已獲授權使用本準則所載核證機關服務者接達，盡可能降低來自網絡的風險。

6.7 加密模組工程控制

香港數碼證書頒發中心使用之加密裝置至少達到 FIPS140-2 第 3 級。

7． 證書、證書撤銷清單

7.1 證書結構

本準則提及之證書內有用於確認電子訊息發送人身分及核實該等訊息是否完整之公開密碼匙（即用於核實數碼簽署之公開密碼匙）。本準則提及之證書一律以 X.509 第三版本之格式發出（見**附錄 B**）。

附錄 D 載有各類香港數碼證書頒發中心數碼證書之特點摘要。

7.2 證書撤銷清單結構

香港數碼證書頒發中心證書撤銷清單之格式為 X.509 第二版本（見**附錄 C**）。

8. 準則管理

本準則之更改一律須經香港數碼證書頒發中心核准及公布。有關準則一經香港數碼證書頒發中心在網頁或香港數碼證書頒發中心儲存庫公布，更改即時生效，並對當時及之後獲發證書的申請人以及登記人均具約束力。就任何對本準則作出的更改，香港數碼證書頒發中心會在實際可行的情況下盡快通知數字政策專員。申請人、登記人及倚據人士可從香港數碼證書頒發中心網頁或香港數碼證書頒發中心儲存庫瀏覽此份準則以及其舊有版本。

附錄 A - 詞彙

除非文意另有所指，否則下列文詞在本準則中釋義如下：

“接受”就某證書而言—

a) 在某人在該證書內指名或識別為獲發給該證書的人的情況下，指—
   (i) 確認該證書包含的關於該人的資訊是準確的；
   (ii) 批准將該證書向他人公布或在某儲存庫內公布；
   (iii) 使用該證書；或
   (iv) 以其他方式顯示承認該證書；或
b) 在某人將會在該證書內指名或識別為獲發給該證書的人的情況下，指—
   (i) 確認該證書將會包含的關於該人的資訊是準確的；
   (ii) 批准將該證書向他人公布或在某儲存庫內公布；或
   (iii) 以其他方式顯示承認該證書；” ；

“申請人”指自然人或法人並已申請數碼證書。

“非對稱密碼系統”指能產生安全配對密碼匙之系統。安全配對密碼匙由用作產生數碼簽署之私人密碼匙及用作核實數碼簽署之公開密碼匙組成。

“獲授權代表”指登記人機構之授權代表。

“授權單位”指登記人機構屬下的單位；而登記人機構已授權該單位使用發出予該登記人機構的數碼證書（保密）的私人密碼匙。

“授權用戶” 指登記人機構之成員或僱員；而登記人機構已授權該成員或僱員使用發出予該登記人機構的數碼證書（機構）的私人密碼匙。成員則指已經與該登記人機構以某種形式維持合法關係的人。

“授權撤銷清單” 列舉獲根源證書在已授權的中繼證書原定到期時間前宣佈無效之公開密碼匙中繼證書之資料。

“核證機關”指向他人(可以為另一核證機關)發出證書者。

“證書”或**“數碼證書”**指符合以下所有說明之紀錄 ：

a) 由核證機關為證明數碼簽署之目的而發出而該數碼簽署用意為確認持有某特定配對密碼匙者身分或其他主要特徵；
b) 識別發出紀錄之核證機關；
c) 指名或識別獲發給紀錄者；
d) 包含該獲發給紀錄者之公開密碼匙；並
e) 經發出紀錄的核證機關簽署。

“核證作業準則”或**“準則”**指核證機關發出以指明其在發出證書時使用之作業實務及標準之準則。

“證書撤銷清單”列舉證書發出人在證書原定到期時間前宣佈無效之公開密碼匙證書（或其他類別證書）之資料。

“合約” 指香港數碼證書頒發中心所批出之香港數碼證書頒發中心核證機關的外判合約，根據本作業準則營運及維持香港數碼證書頒發中心核證機關之服務及系統。

“承辦商”指翹晉電子商務有限公司及其合約分判商（列載於**附錄 F**，若有的話）。其為香港數碼證書頒發中心根據認可核證機關業務守則第 3.2 段所委任之代理人，根據合約條款，為香港數碼證書頒發中心營運及維持香港數碼證書頒發中心核證機關之服務及系統。

“對應”就私人或公開密碼匙而言，指屬同一配對密碼匙。

“業務守則”指由數字政策專員在條例第 33 條下頒佈之認可核證機關業務守則。

“數碼簽署”就電子紀錄而言，指簽署人之電子簽署，該簽署用非對稱密碼系統及雜湊函數將該電子紀錄作數據變換產生，使持有原本未經數據變換之電子紀錄及簽署人之公開密碼匙者能據此確定：
(a) 該數據變換是否用與簽署人之公開密碼匙對應之私人密碼匙產生；以及
(b) 產生數據變換後，原本之電子紀錄是否未經變更。

“數碼證書檔案 USB” 為一種 USB 快閃記憶體，是儲存數碼證書的儲存媒體。最新的數碼證書檔案 USB 價格會在香港數碼證書頒發中心網頁公布。

“數碼證書儲存媒體”指一種儲存媒體，例如數碼證書檔案 USB，用於儲存數碼證書及私人密碼匙。

“數碼證書登記人平台”指由香港數碼證書頒發中心維護的網上平台，供登記人建立帳戶、遞交證書申請、進行付款，以及管理其數碼證書。

“電子紀錄”指資訊系統產生之數碼形式之紀錄，而該紀錄：
(a) 能在資訊系統內傳送或由一個資訊系統傳送至另一個資訊系統；並
(b) 能儲存在資訊系統或其他媒介內。

“電子簽署”指與電子紀錄相連或在邏輯上相聯之數碼形式之字母、字樣、數目字或其他符號，而該等字母、字樣、數目字或其他符號為認證或承認該紀錄之目的定立或採用者。

“身份證” 指由香港特別行政區政府入境事務處發出的香港身份證，包括智能身份證。

“智方便+”指由香港特別行政區政府提供的「智方便」數碼身分平台的增強版本。該版本包含符合《電子交易條例》（第 553 章）要求的數碼簽署功能，使用戶能夠建立具法律效力的數碼簽署。

“資訊”包括資料、文字、影像、聲音編碼、電腦程式、軟件及資料庫。

“資訊系統”指符合以下所有說明之系統：
(a) 處理資訊；
(b) 紀錄資訊；
(c) 能用作使資訊紀錄或儲存在不論位於何處之資訊系統內，或能用作將資訊在該等系統內以其他方式處理；及
(d) 能用作檢索資訊(不論該等資訊紀錄或儲存在該系統內或在不論位於何處之資訊系統內)。

“中介人”就某特定電子紀錄而言，指代他人發出、接收或儲存該紀錄，或就該紀錄提供其他附帶服務者。

“稅務局參考編號”指稅務局根據《稅務條例》(第 112 章)向申報財務機構/申報實體提供的參考編號。稅務局參考編號會於稅務局向申報財務機構/申報實體發出的證明文件內提供。

“發出”就證書而言，指
(a) 製造該證書，然後將該證書包含的關於在該證書內指名或識別為獲發給該證書的人的資訊，通知該人；或
(b) 將該證書將會包含的關於在該證書內指名或識別為獲發給該證書的人的資訊，通知該人，然後製造該證書，然後提供該證書予該人使用；

“配對密碼匙”在非對稱密碼系統中，指私人密碼匙及其在數學上相關之公開密碼匙，而該公開密碼匙可核實該私人密碼匙所產生之數碼簽署。

“條例”指香港法例第 553 章《電子交易條例》。

“個人密碼”指用於保護授權用戶的數碼證書及其私人密碼匙的密碼。

“發訊者”就某電子紀錄而言，指發出或產生該紀錄者，或由他人代為發出或產生該紀錄者，惟不包括中介人。

“PKCS#11 兼容裝置”指一種裝置（例如智能卡），除可儲存數碼證書及支援加密功能外，亦符合由 RSA 實驗室公布的公開密碼匙加密標準 (PKCS)中第 11 項有關加密裝置介面標準的規格，而該裝置應獲得 FIPS 140-2 第三級或以上的認證。

“私人密碼匙”指配對密碼匙中用作產生數碼簽署之密碼匙。

“公開密碼匙”指配對密碼匙中用作核實數碼簽署之密碼匙。

“認可證書”指：
（a） 根據電子交易條例第 22 條認可之證書；
（b） 屬根據電子交易條例第 22 條認可之證書之類型、類別或種類之證書；或
（c） 電子交易條例第 34 條所述核證機關所發出指明為認可證書之證書。

“認可核證機關”指根據《電子交易條例》下的「核證機關認可計劃」獲得認可的核證機關。

“紀錄”指在有形媒界上註記、儲存或以其他方式固定之資訊，亦指儲存在電子或其他媒界可藉理解形式還原之資訊。

“核證登記機關” 指由香港數碼證書頒發中心指定，代表香港數碼證書頒發中心核證機關行使一定職能，並提供香港數碼證書頒發中心核證機關之若干服務之機構。

“倚據人士”，即依賴方，指證書的接收者，依賴於該證書和（或）該證書所驗證的電子簽名。

“倚據限額”指就認可證書倚據而指明之金錢限額。

“儲存庫”指用作儲存並檢索證書以及其他與證書有關資訊之資訊系統。

“負責人員”就某核證機關而言，指在該機關與本條例有關活動中居要職者。

“簽”及**“簽署”**包括由意圖認證或承認紀錄者簽訂或採用之任何符號，或該人使用或採用之任何方法或程序。

“智能身份證” 指可將數碼證書載入其中的**身份證**。

“中繼證書”指由香港數碼證書頒發中心根源證書所發出的中繼核證機關證書，並用於發出香港數碼證書頒發中心認可證書。

“合約分判商”指受翹晉電子商務有限公司委任的機構，執行合約中的部份工作。

“登記人”指符合以下所有說明的人：

(i) 在某證書內指名或識別為獲發給證書；
(ii) 已接受該證書；及
(iii) 持有與列於該證書內的公開密碼匙對應之私人密碼匙；

“登記人協議”指由登記人及香港數碼證書頒發中心訂立的協議，包含在申請表上列明的登記人條款及條件及本核證作業準則的條款。

“登記人機構” 指作為登記人的機構；而其獲授權代表已簽署登記人協議，及根據此核證作業準則，該機構為合資格並獲發出數碼證書之機構。

“穩當系統”指符合以下所有條件之電腦硬體、軟件及程序：
(a) 合理地安全可免遭受入侵及不當使用；
(b) 在可供使用情況、可靠性及操作方式能於合理期內維持正確等方面達到合理水平；
(c) 合理地適合執行其原定功能；及
(d) 依循廣為接受之安全原則。

“主體名稱” 指證書持有者名字的信息。

為執行電子交易條例，如某數碼簽署可參照列於某證書內之公開密碼匙得以核實，而該證書之登記人為簽署人，則該數碼簽署即可視作獲該證書證明。

附錄 B - 香港數碼證書頒發中心數碼證書格式

本附錄詳述由中繼證書 " HKCA d-Cert CA 1 - 25" 及 " HKCA d-Cert CA 1 - 25A" 根據本核證作業準則發出的數碼證書格式。如欲了解由香港數碼證書頒發中心其他中繼證書或根據其他核證作業準則發出的數碼證書格式，請根據數碼證書上的發出日期或「證書政策」內的物件識別碼，查閱相關版本的核證作業準則。

1) 數碼證書（個人）格式

1.1 根源證書 "HKCA Root CA 1" 之下

以下為適用於由中繼證書" HKCA d-Cert CA 1 - 25"發出的數碼證書（個人）:-

欄位名稱		欄位內容	
		數碼證書（個人）	發出予未滿18歲人仕的數碼證書（個人）
標準欄 (Standard fields)			
版本 (Version)		X.509 V3	
序號 (Serial number)		[由香港數碼證書頒發中心系統設置的二十位元組十六進制數字]	
簽署算式識別 (Signature algorithm ID)		Sha256RSA	
發出人 (Issuer)		cn=HKCA d-Cert CA 1 - 25 o= Hong Kong Internet Registration Corporation Limited l=Hong Kong s=Hong Kong c=HK	
有效期 (Validity period)	不早於 (Not before)	[由香港數碼證書頒發中心系統設置的UTC 時間]	
	不遲於 (Not after)	[由香港數碼證書頒發中心系統設置的UTC 時間]	
主體名稱 (Subject name)		cn=[香港身份證姓名]（附註1） e=[電子郵箱地址]（附註2） ou=[登記人參考編號]（附註3） o=HKCA d-Cert (Personal) c=HK	cn=[香港身份證姓名]（附註1） e=[電子郵箱地址]（附註2） ou=[登記人參考編號]（附註3） o= HKCA d-Cert (Personal/Minor)（附註4） c=HK
主體公開密碼匙資料 (Subject public key info)		算式識別 (Algorithm ID)：RSA 公開密碼匙 (Public key)：密碼匙長度為2048位元	
發出人識別名稱 (Issuer unique identifier)		未使用	
登記人識別名稱 (Subject unique identifier)		未使用	
標準延伸欄位 (Standard extension)（附註5）			
機關密碼匙識別名稱 (Authority Key Identifier)	發出人 (Issuer)	cn= HKCA Root CA 1, o= Hong Kong Internet Registration Corporation Limited, l=Hong Kong s=Hong Kong c=HK	
	序號 (Serial number)	[從發出人處獲取]	

欄位名稱		欄位內容	
		數碼證書（個人）	發出予未滿18歲人仕的數碼證書（個人）
密碼匙使用方法 (Key usage)		不可否認，數碼簽署，密碼匙加密 （此欄為“關鍵”欄位）	
證書政策 (Certificate policy)		Policy Identifier = [物件識別碼]（附註 6） Policy Qualifier ID = CPS Qualifier : [核證作業準則的URL]	
主體別名 (Subject alternative name)	DNS	[經加密的香港身份證號碼]（附註10）	
	Rfc822	[證書持有人電子郵箱地址]（附註2）	
發出人別名 (Issuer alternative name)		未使用	
基本限制 (Basic constraints)	主體類型 (Subject type)	最終實體	
	路徑長度限制 (Path length constraint)	無	
延伸密碼匙使用方法 (Extended key usage)		SSL Client, S/MIME	
證書撤銷清單分發點 (CRL distribution point)		分發點名稱 = [證書撤銷清單分發點URL]（附註11）	
Netscape 延伸欄位 (Netscape extension)（附註5）			
Netscape 證書類型 (Netscape cert type)		未使用	
Netscape SSL伺服器名稱 (Netscape SSL server name)		未使用	
Netscape 備註 (Netscape commen		未使用	

以下為適用於由中繼證書" HKCA d-Cert CA 1 - 25A”發出支援 Adobe PDF 簽署的數碼證書（個人）:-

欄位名稱		欄位內容
標準欄 (Standard fields)		
版本 (Version)		X.509 V3
序號 (Serial number)		[由香港數碼證書頒發中心系統設置的二十位元組十六進制數字]
簽署算式識別 (Signature algorithm ID)		Sha256RSA
發出人 (Issuer)		cn=HKCA d-Cert CA 1 - 25A, o= Hong Kong Internet Registration Corporation Limited, l=Hong Kong, s=Hong Kong, c=HK
有效期 (Validity period)	不早於 (Not before)	[由香港數碼證書頒發中心系統設置的UTC 時間]

欄位名稱		欄位內容
	不遲於 (Not after)	[由香港數碼證書頒發中心系統設置的UTC 時間]
主體名稱 (Subject name)		cn=[香港身份證姓名]（附註1） e=[電子郵箱地址]（附註2） ou=[登記人參考編號]（附註3） o= HKCA d-Cert (Personal) c=HK
主體公開密碼匙資料 (Subject public key info)		算式識別 (Algorithm ID)：RSA 公開密碼匙 (Public key)：密碼匙長度為2048位元
發出人識別名稱 (Issuer unique identifier)		未使用
登記人識別名稱 (Subject unique identifier)		未使用
標準延伸欄位 (Standard extension)（附註5）		
機關密碼匙識別名稱 (Authority Key Identifier)	**發出人 (Issuer)**	cn=HKCA Root CA 1, o= Hong Kong Internet Registration Corporation Limited, l=Hong Kong, s=Hong Kong, c=HK
	序號 (Serial number)	[從發出人處獲取]
密碼匙使用方法 (Key usage)		不可否認，數碼簽署 **（此欄為“關鍵”欄位）**
證書政策 (Certificate policy)		Policy Identifier = [物件識別碼]（附註 6） Policy Qualifier ID = CPS Qualifier : [核證作業準則的URL] Policy Identifier =1.3.6.1.4.1.64092.1.4 (Note 9) Policy Qualifier Id = CPS Qualifier : [核證作業準則的URL]
主體別名 (Subject alternative name)	**DNS**	[經加密的香港身份證號碼]（附註10）
	Rfc822	[證書持有人電子郵箱地址]（附註2）
發出人別名 (Issuer alternative name)		未使用
基本限制 (Basic constraints)	**主體類型 (Subject type)**	最終實體
	路徑長度限制 (Path length constraint)	無
延伸密碼匙使用方法 (Extended key usage)		SSL Client, S/MIME
證書撤銷清單分發點 (CRL distribution point)		分發點名稱 = [證書撤銷清單分發點URL]（附註12）
Netscape 延伸欄位 (Netscape extension)（附註5）		
Netscape 證書類型 (Netscape cert type)		未使用

欄位名稱		欄位內容
Netscape SSL伺服器名稱 (Netscape SSL server name)		未使用
Netscape 備註 (Netscape commen		未使用

附註:

1. 申請人姓名格式: 英文格式 - 姓氏（大寫）+ 名 （例如 CHAN Tai Man David）
2. 申請人所提供的電子郵箱地址（如沒有電子郵箱地址，此欄將會留空），該電子郵箱地址未經核實。
3. 登記人參考編號： 10 位數字
4. “d-Cert (Personal/Minor)” 表示 申請人於獲發出證書時未滿 18 歲（見本核證作業準則第 3.1.1.2 條）.
5. 除非另外註明，所有標準延伸欄位及 Netscape 延伸欄位均為 “非關鍵” (Non-Critical) 延伸欄位。
6. 本欄已包括本核證作業準則的物件識別碼 (Object Identifier, OID)。關於本準則的物件識別碼，請參閱本準則第 1.1 條。
7. 保留作將來使用。
8. 保留作將來使用。
9. 本欄已增加一個支援 Adobe PDF 簽名的物件識別碼。
10. 申請人的香港身份證號碼(包括括號內的數字)(以 **hkid_number** 表示)將會經申請人的私人密碼匙簽署並轉化為一雜湊數值(以 **cert_hkid_hash** 表示)後，存入證書：

$$\text{cert\_hkid\_hash} = \textit{SHA-1}\,(\,\textit{RSA}_{\textit{privatekey, sha-1}}\,(\,\text{hkid\_number}\,)\,)$$

*SHA-1*為一雜湊函數而*RSA*則為簽署函數

在代製密碼匙的過程中，**hkid_number** 則會在香港數碼證書頒發中心處所內代製密碼時簽署，並產生已簽署的香港身份證號碼的雜湊數值 $\textit{SHA-1}\,(\,\textit{RSA}_{\textit{privatekey, sha-1}}\,(\,\text{hkid\_number}\,)\,)$，該雜湊數值會輸入證書內的指定延伸欄位。

11. 證書撤銷清單分發點 URL 為 http://crl1.hkca.hk/crl/dCertCA1-25CRL_<xxxxx>.crl，由中繼證書"HKCA d-Cert CA 1 - 25"所發出，其中 <xxxxx> 為經香港數碼證書頒發中心系統產生，包含 5 個數字或字符的字串。香港數碼證書頒發中心會公布各「分割式證書撤銷清單」。已暫時吊銷或撤銷證書的資料，會在該證書 “證書撤銷清單分發點” 欄位內註明的已分割證書撤銷清單內公布。
12. 證書撤銷清單分發點 URL 為 http://crl1.hkca.hk/crl/dCertCA1-25ACRL_<xxxxx>.crl，由中繼證書"HKCA d-Cert CA 1 - 25A "所發出，其中 <xxxxx> 為經香港數碼證書頒發中心系統產生，包含 5 個數字或字符的字串。香港數碼證書頒發中心會公布各「分割式證書撤銷清單」。已暫時吊銷或撤銷證書的資料，會在該證書 “證書撤銷清單分發點” 欄位內註明的已分割證書撤銷清單內公布。

2) 數碼證書（機構）格式

2.1 根源證書 “HKCA Root CA 1” 之下

以下為適用於由中繼證書" HKCA d-Cert CA 1 - 25”發出的數碼證書（機構）:-

欄位名稱		欄位內容
標準欄 (Standard fields)		
版本 (Version)		X.509 V3
序號 (Serial number)		[由香港數碼證書頒發中心系統設置的二十位元組十六進制數字]
簽署算式識別 (Signature algorithm ID)		sha256RSA
發出人 (Issuer)		cn=HKCA d-Cert CA 1 - 25, o= Hong Kong Internet Registration Corporation Limited, l=Hong Kong, s=Hong Kong, c=HK
有效期 (Validity period)	不早於 (Not before)	[由香港數碼證書頒發中心系統設置的UTC 時間]
	不遲於 (Not after)	[由香港數碼證書頒發中心系統設置的UTC 時間]
主體名稱 (Subject name)		cn=[授權用戶姓名]（附註1） e=[電子郵箱地址]（附註2） ou=[登記人參考編號]（附註3） ou=[(商業登記證書編號或稅務局參考編號)+註冊證書/登記證書編號+其他]（附註4） ou=[登記人機構名稱]（附註5） ou=[登記人機構分行/部門名稱]（附註5） o=HKCA d-Cert (Organisational) c=HK
主體公開密碼匙資料 (Subject public key info)		算式識別 (Algorithm ID)：RSA 公開密碼匙 (Public key)：密碼匙長度為2048位元
發出人識別名稱 (Issuer unique identifier)		未使用
登記人識別名稱 (Subject unique identifier)		未使用
標準延伸欄位 (Standard extension)（附註6）		
機關密碼匙識別名稱 (Authority Key Identifier)	發出人 (Issuer)	cn= HKCA Root CA 1, o=Hong Kong Internet Registration Corporation Limited, l=Hong Kong, s=Hong Kong, c=HK
	序號 (Serial number)	[從發出人處獲取]
密碼匙使用方法 (Key usage)		不可否認，數碼簽署，密碼匙加密 **（此欄為“關鍵”欄位）**
證書政策 (Certificate policy)		Policy Identifier =[物件識別碼]（附註 7） Policy Qualifier ID = CPS Qualifier : [核證作業準則的URL]
主體別名 (Subject alternative name)	DNS	[0-10特定應用編碼]（附註10）
	第一目錄名稱 (First Directory Name)	ou=[登記人機構中文名稱]（附註5） ou=[登記人機構分行/部門中文名稱]（附註5）

欄位名稱		欄位內容
	Rfc822	[證書持有人電子郵箱地址]（附註2）
發出人別名 (Issuer alternative name)		未使用
基本限制 (Basic constraints)	主體類型 (Subject type)	最終實體
	路徑長度限制 (Path length constraint)	無
延伸密碼匙使用方法 (Extended key usage)		SSL client, S/MIME
證書撤銷清單分發點 (CRL distribution point)		分發點名稱 = [證書撤銷清單分發點URL]（附註11）
Netscape 延伸欄位 (Netscape extension)（附註6）		
Netscape 證書類型 (Netscape cert type)		未使用
Netscape SSL伺服器名稱 (Netscape SSL server name)		未使用
Netscape 備註 (Netscape comment)		未使用

以下為適用於由中繼證書" HKCA d-Cert CA 1 - 25A”發出支援 Adobe PDF 簽署的數碼證書（機構 ）:-

欄位名稱		欄位內容
標準欄 (Standard fields)		
版本 (Version)		X.509 V3
序號 (Serial number)		[由香港數碼證書頒發中心系統設置的二十位元組十六進制數字]
簽署算式識別 (Signature algorithm ID)		sha256RSA
發出人 (Issuer)		cn=HKCA d-Cert CA 1 - 25A, o=Hong Kong Internet Registration Corporation Limited, l=Hong Kong, s=Hong Kong, c=HK
有效期 (Validity period)	不早於 (Not before)	[由香港數碼證書頒發中心系統設置的UTC 時間]
	不遲於 (Not after)	[由香港數碼證書頒發中心系統設置的UTC 時間]
主體名稱 (Subject name)		cn=[授權用戶姓名]（附註1） e=[電子郵箱地址]（附註2） ou=[登記人參考編號]（附註3） ou=[(商業登記證書編號或稅務局參考編號)+註冊證書/登記證書編號+其他]（附註4） ou=[登記人機構名稱]（附註5） ou=[登記人機構分行/部門名稱]（附註5） o= HKCA d-Cert (Organisational) c=HK
主體公開密碼匙資料 (Subject public key info)		算式識別 (Algorithm ID)：RSA 公開密碼匙 (Public key)：密碼匙長度為2048位元
發出人識別名稱 (Issuer unique identifier)		未使用
登記人識別名稱 (Subject unique identifier)		未使用
標準延伸欄位 (Standard extension)（附註6）		

欄位名稱		欄位內容
機關密碼匙識別名稱 (Authority Key Identifier)	**發出人 (Issuer)**	cn=HKCA Root CA 1, o=Hong Kong Internet Registration Corporation Limited, l=Hong Kong, s=Hong Kong, c=HK
	序號 (Serial number)	[從發出人處獲取]
密碼匙使用方法 (Key usage)		不可否認，數碼簽署 **（此欄為“關鍵”欄位）**
證書政策 (Certificate policy)		Policy Identifier =[物件識別碼]（附註 7） Policy Qualifier ID = CPS Qualifier : [核證作業準則的URL] Policy Identifier = 1.3.6.1.4.1.64092.1.4 (附註9) Policy Qualifier Id = CPS Qualifier : [核證作業準則的URL]
主體別名 (Subject alternative name)	DNS	[0-10特定應用編碼]（附註10）
	第一目錄名稱 (First Directory Name)	ou=[登記人機構中文名稱]（附註5） ou=[登記人機構分行/部門中文名稱]（附註5）
	Rfc822	[證書持有人電子郵箱地址]（附註2）
發出人別名 (Issuer alternative name)		未使用
基本限制 (Basic constraints)	**主體類型 (Subject type)**	最終實體
	路徑長度限制 (Path length constraint)	無
延伸密碼匙使用方法 (Extended key usage)		SSL client, S/MIME
證書撤銷清單分發點 (CRL distribution point)		分發點名稱 = [證書撤銷清單分發點URL]（附註12）
Netscape 延伸欄位 (Netscape extension)（附註6）		
Netscape 證書類型 (Netscape cert type)		未使用
Netscape SSL伺服器名稱 (Netscape SSL server name)		未使用
Netscape 備註 (Netscape comment)		未使用

附註:

1. 授權用戶姓名格式: 英文格式 - 姓氏（大寫）+ 名 （例如 CHAN Tai Man David）
2. 授權用戶所提供的電子郵箱地址（如沒有電子郵箱地址，此欄將會留空），該電子郵箱地址未經核實。
3. 登記人參考編號： 10 位數字
4. “商業登記證書編號”欄位 : 一串 16 位數字/字母【如無商業登記證書編號，欄位全部為零(“0”)】。如機構提交由稅務局發出的證明文件副本，以代替商業登記證副本，則“商業登記證書編號”欄位會包括由證明文件提供的一串 8 位數字/字母之稅務局參考編號連同後導的 8 個零("0")。“註冊證書 / 登記證書”欄位 : 一串 8 位數字/字母【如註冊證書 / 登記證書編號少於 8 位數字/字母，編號前導零(“0”)，如無註冊證書 / 登記證書編號，欄位全部為零(“0”)，如是"有限合夥基金"，欄位全部為零(“0”)】, “其他”欄位: 一串最多 30 位數字/字母 (如有)。香港特別行政區政府部門之“商業登記編號”及“註冊證書 / 登記證書”欄位全部為零(“0”)，部門簡稱 (例如 HKPO 代表香港數碼證書頒發中心)會放入“其他” 欄位。根據《有限合夥基金條例》(第 637 章) 註冊為"有限合夥基金"的機構，其註冊證明書編號會放入“其他” 欄位。

5. 只有中文名稱作登記之機構，預設的名稱「***CHINESE NAME ONLY***」將被設定為機構的英文名稱。在任何情況下當登記人機構提供了中文名稱並經香港數碼證書頒發中心核實,其名稱會於主體別名的第一目錄名稱 (First Directory Name)欄位內顯示（見本核證作業準則第 3.1.1.6 條）。機構中文名稱須採用 ISO/IEC 10646 國際編碼標準。
6. 除非另外註明，所有標準延伸欄位及 Netscape 延伸欄位均為 “非關鍵” (Non-Critical) 延伸欄位。
7. 本欄已包括本核證作業準則的物件識別碼 (Object Identifier, OID)。關於本準則的物件識別碼，請參閱本準則第 1.1 條。
8. 保留作將來使用。
9. 本欄已增加一個支援 Adobe PDF 簽名的物件識別碼。
10. 特定應用中之特定應用編碼會在此欄位進行定義。（見**附錄 H**）
11. 證書撤銷清單分發點 URL 為 http://crl1.hkca.hk/crl/dCertCA1-25CRL_**<xxxxx>.crl**，由中繼證書"HKCA d-Cert CA 1 - 25"所發出，其中 <xxxxx> 為經香港數碼證書頒發中心系統產生，包含 5 個數字或字符的字串。香港數碼證書頒發中心會公布各「分割式證書撤銷清單」。已暫時吊銷或撤銷證書的資料，會在該證書 “證書撤銷清單分發點” 欄位內註明的已分割證書撤銷清單內公布。
12. 證書撤銷清單分發點 URL 為 http://crl1.hkca.hk/crl/dCertCA1-25ACRL_<xxxxx>.crl，由中繼證書"HKCA d-Cert CA 1 - 25A "所發出，其中 <xxxxx> 為經香港數碼證書頒發中心系統產生，包含 5 個數字或字符的字串。香港數碼證書頒發中心會公布各「分割式證書撤銷清單」。已暫時吊銷或撤銷證書的資料，會在該證書 “證書撤銷清單分發點” 欄位內註明的已分割證書撤銷清單內公布。

3) 數碼證書（保密）格式

3.1 根源證書 “HKCA Root CA 1” 之下

以下為適用於由中繼證書" HKCA d-Cert CA 1 - 25”發出的數碼證書（ 保密 ）:-

欄位名稱		欄位內容
標準欄 (Standard fields)		
版本 (Version)		X.509 V3
序號 (Serial number)		[由香港數碼證書頒發中心系統設置的二十位元組十六進制數字]
簽署算式識別 (Signature algorithm ID)		sha256RSA
發出人 (Issuer)		cn=HKCA d-Cert CA 1 - 25, o=Hong Kong Internet Registration Corporation Limited, l=Hong Kong, s=Hong Kong, c=HK
有效期 (Validity period)	不早於 (Not before)	[由香港數碼證書頒發中心系統設置的UTC 時間]
	不遲於 (Not after)	[由香港數碼證書頒發中心系統設置的UTC 時間]
主體名稱 (Subject name)		cn=[授權單位名稱]（附註1） e=[電子郵箱地址]（附註2） ou=[登記人參考編號]（附註3） ou=[商業登記證書編號+註冊證書/登記證書編號+其他]（附註4） ou=[登記人機構名稱]（附註5） ou=[登記人機構分行/部門名稱]（附註5） o=HKCA d-Cert (Encipherment) c=HK
主體公開密碼匙資料 (Subject public key info)		算式識別 (Algorithm ID)：RSA 公開密碼匙 (Public key)：密碼匙長度為2048位元
發出人識別名稱 (Issuer unique identifier)		未使用
登記人識別名稱 (Subject unique identifier)		未使用
標準延伸欄位 (Standard extension)（附註6）		
機關密碼匙識別名稱 (Authority Key Identifier)	發出人 (Issuer)	cn=HKCA Root CA 1, o=Hong Kong Internet Registration Corporation Limited, l=Hong Kong, s=Hong Kong, c=HK
	序號 (Serial number)	[從發出人處獲取]
密碼匙使用方法 (Key usage)		數碼簽署，密碼匙加密 **（此欄為 “關鍵” 欄位）**
證書政策 (Certificate policy)		Policy Identifier = [物件識別碼]（附註 7） Policy Qualifier ID = CPS Qualifier : [核證作業準則的URL]
主體別名 (Subject alternative name)	DNS	未使用
	Rfc822	[證書持有人電子郵箱地址]（附註2）
發出人別名 (Issuer alternative name)		未使用

欄位名稱		欄位內容
基本限制 (Basic constraints)	**主體類型 (Subject type)**	最終實體
	路徑長度限制 (Path length constraint)	無
延伸密碼匙使用方法 (Extended key usage)		SSL Client, S/MIME
證書撤銷清單分發點 (CRL distribution point)		**分發點名稱 = [證書撤銷清單分發點URL]** （附註8）
Netscape 延伸欄位 (Netscape extension)（附註6）		
Netscape 證書類型 (Netscape cert type)		未使用
Netscape SSL伺服器名稱 (Netscape SSL server name)		未使用
Netscape 備註 (Netscape comment)（附註9）		未使用

附註:

1. 登記人機構之授權單位名稱
2. 授權單位代表所提供的電子郵箱地址
3. 登記人參考編號： 10 位數字
4. “商業登記證書編號” 欄位 : 一串 16 位數字/字母【如無商業登記證書編號，欄位全部為零(“0”)】, “註冊證書 / 登記證書” 欄位 : 一串 8 位數字/字母【如註冊證書 / 登記證書編號少於 8 位數字/字母，編號前導零(“0”)，如無註冊證書 / 登記證書編號，欄位全部為零(“0”)， 如是"有限合夥基金"，欄位全部為零(“0”)】, “其他” 欄位: 一串最多 30 位數字/字母 (如有)。香港特別行政區政府部門之 “商業登記編號” 及 “註冊證書 / 登記證書” 欄位全部為零(“0”)，部門簡稱 (例如 HKPO 代表香港數碼證書頒發中心)會放入 “其他” 欄位。根據《有限合夥基金條例》(第 637 章) 註冊為"有限合夥基金"的機構，其註冊證明書編號會放入 “其他” 欄位。
5. 只有中文名稱或只提供中文名稱作登記之機構，其名稱不會在此欄內顯示 (見本核證作業準則第 3.1.1.6 條)。
6. 除非另外註明，所有標準延伸欄位及 Netscape 延伸欄位均為 “非關鍵” (Non-Critical) 延伸欄位。
7. 本欄已包括本準則的物件識別碼 (Object Identifier, OID)。關於本準則的物件識別碼，請參閱本準則第 1.1 條。
8. 證書撤銷清單分發點 URL 為 http://crl1.hkca.hk/crl/dCertCA1-25CRL_<xxxxx>.crl，由中繼證書"HKCA d-Cert CA 1 - 25A "所發出，其中 <xxxxx> 為經香港數碼證書頒發中心系統產生，包含 5 個數字或字符的字串。香港數碼證書頒發中心會公布各「分割式證書撤銷清單」已暫時吊銷或撤銷證書的資料，會在該證書 “證書撤銷清單分發點” 欄位內註明的已分割證書撤銷清單內公布。

附錄 C - 香港數碼證書頒發中心證書撤銷清單 (CRL) 及香港數碼證書頒發中心授權撤銷清單 (ARL)格式

本附錄 C 詳述有關由中繼證書" HKCA d-Cert CA 1 - 25"及"HKCA d-Cert CA 1 – 25A"所發出的證書撤銷清單，以及由根源證書" HKCA Root CA 1"所發出的授權撤銷清單的更新及公布安排和其格式。

香港數碼證書頒發中心每天三次更新及公布下述的證書撤銷清單（更新時間為香港時間 09:15、14:15 及 19:00（即格林尼治平時[GMT 或 UTC] 時間 01:15、06:15 及 11:00））；證書撤銷清單載有根據本核證作業準則而暫時吊銷或撤銷的數碼證書的資訊：

a) **「分割式證書撤銷清單」(Partitioned CRL)** 包含分組的已暫時吊銷或已撤銷證書的資料。公眾可於下述位址(URL)獲取相關的「分割式證書撤銷清單」：

   i. 由中繼證書"HKCA d-Cert CA 1 - 25"所發出數碼證書（個人），數碼證書（機構）及數碼證書（保密）：
   http://crl1.hkca.hk/crl/d-CertCA1-25CRL_<xxxxx>.crl
   其中 <xxxxx> 為包含 5 個數字或字符的字串。

   ii. 由中繼證書" HKCA d-Cert CA 1 – 25A"所發出支援 Adobe PDF 簽署的數碼證書（個人）及數碼證書（機構）：
   http://crl1.hkca.hk/crl/d-CertCA1-25ACRL_<xxxxx>.crl
   其中 <xxxxx> 為包含 5 個數字或字符的字串。

b) **「整體證書撤銷清單」(Full CRL)** 包含分別由中繼證書" HKCA d-Cert CA 1 - 25"，" HKCA d-Cert CA 1 – 25A"所發出的所有已暫時吊銷或已撤銷證書的資料。公眾可分別於下述位址(URL)獲取「整體證書撤銷清單」：

   i. 由中繼證書" HKCA d-Cert CA 1 - 25"所發出的證書：
   http://crl1.hkca.hk/crl/d-CertCA1-25CRL.crl 或
   ldap://ldap1.hkca.hk (port 389, cn=HKCA d-Cert CA 1 - 25 CRL, o=Hong Kong Internet Registration Corporation Limited, c=HK)

   ii. 由中繼證書"HKCA d-Cert CA 1 – 25A"所發出的證書：
   http://crl1.hkca.hk/crl/d-CertCA1-25ACRL.crl 或
   ldap://ldap1.hkca.hk (port 389, cn=HKCA d-Cert CA 1 - 25A CRL, o=Hong Kong Internet Registration Corporation Limited, c=HK)

上述的證書撤銷清單包含已暫時吊銷或已撤銷證書的資料，公眾可於證書的「證書撤銷清單分發點」(CRL distribution point) 欄位內註明的位址(URL)獲取相關的證書撤銷清單。

在正常情況下，香港數碼證書頒發中心會於更新時間後，盡快將最新的證書撤銷清單公布。在不能預見及有需要的情況下，香港數碼證書頒發中心可不作事前通知而更改上述證書撤銷清單的更新及公布的時序。香港數碼證書頒發中心也會在有需要及不作事前通知的情況下，於香港數碼證書頒發中心網頁公布補充證書撤銷清單。

香港數碼證書頒發中心會更新及公布授權撤銷清單，而清單內載有已暫時吊銷或已撤銷的中繼證書的資

料。香港數碼證書頒發中心會每年在其下次更新日期前或在有需要時更新及公布。最新發出的授權撤銷清單可於下述位置下載：

i. 根源證書" HKCA Root CA 1"所發出的中繼證書
http://crl1.hkca.hk/crl/RootCA1ARL.crl 或
ldap://ldap1.hkca.hk (port 389, cn=HKCA Root CA 1, o=Hong Kong Internet Registration Corporation Limited, c=HK)

（I） 由中繼證書" HKCA d-Cert CA 1 - 25"根據本準則發出的分割式及整體證書撤銷清單格式:-

標準欄位 (Standard Fields)	子欄位 (Sub-fields)	分割式證書撤銷清單欄位內容	整體證書撤銷清單欄位內容	備註
版本 (Version)		v2		此欄顯示證書撤銷清單格式的版本為 X.509 第二版
簽署算式識別 (Signature algorithm ID)		sha256RSA		此欄顯示用以簽署證書撤銷清單的算法的識別碼
發出人 (Issuer name)		cn=HKCA d-Cert CA 1 - 25, o=Hong Kong Internet Registration Corporation Limited, l=Hong Kong, s=Hong Kong, c=HK		此欄顯示簽署及發出證書撤銷清單的機構
此次更新 (This update)		[UTC 時間]		此欄顯示本證書撤銷清單的發出日期 (是次更新)
下次更新 (Next update)		[UTC 時間]		表示下次證書撤銷清單將於顯示的日期或之前發出 (下次更新)，而不會於顯示的日期之後發出。根據核證作業準則的規定，證書撤銷清單是每天更新及發出
撤銷證書 (Revoked certificates)	用戶證書 (User certificate)	[證書序號]		此欄列出已撤銷證書的證書序號
	撤銷日期 (Revocation date)	[UTC 時間]		此欄顯示撤銷證書的時間
	證書撤銷清單資料延伸欄位 (CRL entry extensions)			
	原因代碼 (Reason code)	[撤銷理由識別碼]		（附註 1）
標準延伸欄位 (Standard extension) （附註 2）				
機關密碼匙識別名稱 (Authority Key Identifier)		[證書撤銷清單發出人主體密碼匙識別名稱]		
證書撤銷清單號碼 (CRL number)		[由核證系統產生]		此欄顯示證書撤銷清單的編號，該編號以順序形式產生。
發出人分發點 (Issuer distribution point)		[以 DER 方式編碼的證書撤銷清單分發點 (Encoded CRL Distribution Point)] **（此欄為 “關鍵” 欄位）**	[未使用]	本欄位祇為分割式證書撤銷清單使用。

（II） 由中繼證書"HKCA d-Cert CA 1 – 25A"根據本準則發出的分割式及整體證書撤銷清單格式:-

標準欄位 (Standard Fields)	子欄位 (Sub-fields)	分割式證書撤銷清單欄位內容	整體證書撤銷清單欄位內容	備註
版本 (Version)		v2		此欄顯示證書撤銷清單格式的版本為 X.509 第二版
簽署算式識別 (Signature algorithm ID)		sha256RSA		此欄顯示用以簽署證書撤銷清單的算法的識別碼
發出人 (Issuer name)		cn=HKCA d-Cert CA 1 - 25A, o=Hong Kong Internet Registration Corporation Limited, l=Hong Kong, s=Hong Kong, c=HK		此欄顯示簽署及發出證書撤銷清單的機構
此次更新 (This update)		[UTC 時間]		此欄顯示本證書撤銷清單的發出日期 (是次更新)
下次更新 (Next update)		[UTC 時間]		表示下次證書撤銷清單將於顯示的日期或之前發出 (下次更新)，而不會於顯示的日期之後發出。根據核證作業準則的規定，證書撤銷清單是每天更新及發出
撤銷證書 (Revoked certificates)	用戶證書 (User certificate)	[證書序號]		此欄列出已撤銷證書的證書序號
	撤銷日期 (Revocation date)	[UTC 時間]		此欄顯示撤銷證書的時間
	證書撤銷清單資料延伸欄位 (CRL entry extensions)			
	原因代碼 (Reason code)	[撤銷理由識別碼]		（附註 1）
標準延伸欄位 (Standard extension) （附註 2）				
機關密碼匙識別名稱 (Authority Key Identifier)		[證書撤銷清單發出人主體密碼匙識別名稱]		
證書撤銷清單號碼 (CRL number)		[由核證系統產生]		此欄顯示證書撤銷清單的編號，該編號以順序形式產生。
發出人分發點 (Issuer distribution point)		[以 DER 方式編碼的證書撤銷清單分發點 (Encoded CRL Distribution Point)] **（此欄為“關鍵”欄位）**	[未使用]	本欄位祇為分割式證書撤銷清單使用。

(III) 由根證書" HKCA Root CA 1"根據本準則發出的授權撤銷清單格式:-

標準欄位 (Standard fields)	子欄位 (Sub-fields)	授權撤銷清單欄位內容	備註
版本 (Version)		v2	此欄顯示授權撤銷清單格式的版本為 X.509 第二版
簽署算式識別 (Signature algorithm ID)		sha256RSA	此欄顯示用以簽署授權撤銷清單的算法的識別碼
發出人 (Issuer name)		cn=HKCA Root CA 1 o=Hong Kong Internet Registration Corporation Limited, l=Hong Kong, s=Hong Kong, c=HK	此欄顯示簽署及發出授權撤銷清單的機構

標準欄位 (Standard fields)	子欄位 (Sub-fields)	授權撤銷清單欄位內容	備註
此次更新 (This update)		[UTC 時間]	此欄顯示本授權撤銷清單的發出日期 (是次更新)
下次更新 (Next update)		[UTC 時間]	表示下次授權撤銷清單將於顯示的日期或之前發出 (下次更新)，而不會於顯示的日期之後發出。根據核證作業準則的規定，授權撤銷清單是每年更新及發出
撤銷證書 (Revoked certificates)	用戶證書 (User certificate)	[證書序號]	此欄列出已撤銷證書的證書序號
	撤銷日期 (Revocation date)	[UTC 時間]	此欄顯示撤銷證書的時間
	證書撤銷清單資料延伸欄位 (CRL entry extensions)		
	原因代碼 (Reason code)	[撤銷理由識別碼]	（附註 1）
標準延伸欄位 (Standard extension) （附註 2）			
機關密碼匙識別名稱 (Authority Key Identifier)		[授權撤銷清單發出人主體密碼匙識別名稱]	
證書撤銷清單號碼 (CRL number)		[由核證系統產生]	此欄顯示授權撤銷清單的編號，該編號以順序形式產生。
發出人分發點 (Issuer distribution point)		只存有用户證書 =否 只存有核證機關證書=是 間接的 CRL=否 **（此欄為“關鍵”欄位）**	

附註:

1. 以下為可於撤銷證書欄位下列出的理由識別碼：

   0 = 未註明；1 = 密碼資料外洩；2 = 核證機關資料外洩；3 = 聯號變更；
   4 = 證書被取代；5 = 核證機關終止運作；6 = 證書被暫時吊銷

   由於登記人無須提供撤銷證書的原因，所以「原因代碼」會以「0」表示（即「未註明」）。

2. 除非另外註明，所有標準延伸欄位均為 “非關鍵” (Non-Critical) 延伸欄位。

附錄 D - 香港數碼證書頒發中心數碼證書 – 服務摘要

1) 數碼證書（個人）

要點	數碼證書(個人)	數碼證書（個人） 支援 Adobe PDF 簽署	發出予未滿 18 歲人仕的 數碼證書(個人)
登記人	持有有效香港身份證及年滿 18 歲人仕		持有有效香港身份證及未滿 18 歲人仕
依據限額	HK$200,000		HK$0
認可證書	是		
配對密碼匙長度	2048 位元 RSA		
產生配對密碼匙	由香港數碼證書頒發中心代製產生		
核對身分	核對申請人的身分		
證書用途	數碼簽署及數據加密		
證書內包含登記人的資料	• 香港身份證上列出的英文姓名； • 香港身份證號碼的雜湊數值 (hash value)； • 電郵地址；及 • 登記人參考編號（由香港數碼證書頒發中心核證機關系統產生）		
登記費用	見本核證作業準則第 2.4 條		
證書有效期	一年或二年或三年 （見本核證作業準則第 1.2.4 及 3.2 條）		

2) 數碼證書（機構）及數碼證書(保密)

要點	數碼證書(機構)	數碼證書(機構 支援 Adobe PDF 簽署	數碼證書(保密)
登記人	獲香港特別行政區政府發出有效商業登記證之機構（附註 1）、獲香港法例認可之本港法定團體及香港特別行政區政府政策局、部門或機關		
證書持有人	登記人機構之成員或僱員並為授權用戶		登記人機構之授權單位
依據限額	HK$200,000		
認可證書	是		
配對密碼匙長度	2048 位元 RSA		
產生配對密碼匙	由香港數碼證書頒發中心代製產生		
核對身分	核對機構及其獲授權代表的身分		
證書用途	數碼簽署及數據加密		祇作數據加密之用
證書內包含登記人的資料	▪ 登記人機構名稱，包括其中文名稱（如有提供） ▪ 授權用戶英文姓名及其電郵地址 ▪ 登記人參考編號（由香港數碼證書頒發中心系統產生） ▪ 登記人機構之公司 / 商業登記資訊（附註 2）		▪ 登記人機構名稱 ▪ 授權單位英文名稱及其電郵地址 ▪ 登記人參考編號（由香港數碼證書頒發中心系統產生） ▪ 登記人機構之公司 / 商業登記資訊
登記及行政費用	見本核證作業準則第 2.4 條		
證書有效期	一年或二年	一年或二年或三年	一年或二年或三年
	（見本核證作業準則第 1.2.4 及 3.3.2 條）		

附註:

1. 持有由香港特別行政區政府稅務局根據《稅務條例》(第 112 章)發出的有效證明文件的申報財務機構/申報實體，亦可以成為數碼證書（機構）的登記人（見第 1.2.3.2 條）。
2. 持有由香港特別行政區政府稅務局根據《稅務條例》(第 112 章) 發出的有效證明文件的申報財務機構/申報實體，數碼證書只會顯示其稅務局參考編號。

附錄 E - 香港數碼證書頒發中心數碼證書核證登記機關名單

由本核證作業準則生效日期起，香港數碼證書頒發中心數碼證書並無指定之核證登記機關。

附錄 F - 香港數碼證書頒發中心數碼證書服務 - 翹晉電子商務有限公司之合約分判商名單（若有的話）

由本核證作業準則生效日期起，就此核證作業準則而言，香港數碼證書頒發中心數碼證書服務並無指定之受翹晉電子商務有限公司委任的合約分判商。

附錄 G - 核證機關根源證書的有效期

根源證書名稱	有效期	備註
HKCA Root CA 1	2025年10月20日 至 2050年10月14日	
HKCA d-Cert CA 1 - 25	[TBC]	此中繼證書由20XX年X月X日起開始發出認可證書給申請者。
HKCA d-Cert CA 1 - 25A	[TBC]	此中繼證書由20XX年X月X日起開始發出認可證書給申請者。

附錄 H - 香港數碼證書頒發中心數碼證書特定應用名單及相對應之特定應用編碼

由本核證作業準則生效日期起，香港數碼證書頒發中心數碼證書並無特定應用編碼。

附錄 I - RFC3647 與本核證作業準則之比較表

免責聲明：下方比較表旨在為本核證作業準則與 RFC3647 核證作業準則概要之間的相互參考提供便利。若本核證作業準則與 RFC3647 核證作業準則概要之間存在任何語義衝突，概以本核證作業準則的條文為準；如登記人或任何倚據人士因此等語義衝突或因其倚據下方的比較表而遭受任何損失及損害，香港數碼證書頒發中心概不負責。

為免生疑問，如比較表中有註明“不適用”的，主要是因為香港數碼證書頒發中心沒有提供那些作業 / 服務或它們和香港數碼證書頒發中心現有的作業 / 服務無關。

RFC3647 的章節	本準則的相關章節	說明
1. 概括性描述	1	
1.1　概述	1.1	
1.2　文檔名稱與標識	1.1	
1.3　電子認證活動參與者	1.2	
1.3.1 電子認證服務機構	1.2.1	
1.3.2 註冊機構	2.1.2 及附錄 E	
1.3.3 登記人	1.2.2 及 1.2.3	
1.3.4 倚據人士	1.2.2	
1.3.5 其他參與者	2.1.3 及附錄 F	
1.4　證書應用	1.2.3	
1.4.1 適合的證書應用		
1.4.2 限制的證書應用		
1.5　策略管理	前言及 8	
1.5.1 策略文檔管理機構	前言及 8	
1.5.2 聯繫人	1.3	
1.5.3 決定 CPS 符合策略的機構	前言及 8	
1.5.4 CPS 批准程式	8	
1.6　定義和縮寫	附錄 A	
2. 信息發佈與信息管理	2.1.1 及 2.5	
2.1 核准使用證書儲存庫內的資料	2.5.4	
2.2　認證信息的發佈	2.5	
2.3　發佈的時間或頻率	2.5	
2.4　信息庫存取控制	2.5.1 及 2.5.2	
3. 身份標識與鑒別	3	
3.1　命名	3.1	
3.1.1 名稱類型	3.1.1	
3.1.2 對名稱意義化的要求	3.1.2	

RFC3647 的章節	本準則的相關章節	說明
3.1.3 登記人的匿名或偽名	不適用	本準則不接受登記人匿名或偽名
3.1.4 理解不同名稱形式的規則	3.1.3	
3.1.5 名稱的唯一性	3.1.4	
3.1.6 商標的識別、鑒別和角色	3.1.5 及 3.1.6	
3.2 初始身份確認	3.1	
3.2.1 證明擁有私人密碼匙之方法	3.1.7	
3.2.2 組織機構身份的鑒別	3.1.8	
3.2.3 個人身份的鑒別	3.1.9	
3.2.4 沒有驗證的登記人資訊	不適用	本準則參照 RFC2527 制定，不披露此部分內容或僅在附錄 B 中註明
3.2.5 授權確認	3.1.9	
3.2.6 互操作準則	1.1	
3.3 密碼匙更新請求的標識與鑒別	3.3 至 3.4	證書密碼匙將於證書續期過程中被更新
3.3.1 常規密碼匙更新的標識與鑒別	3.3 至 3.4	
3.3.2 撤銷後密碼匙更新的標識與鑒別	3.3 至 3.4	
3.4 撤銷請求的標識與鑒別	4.6.2	
4. 證書生命週期操作要求	4	
4.1 證書申請	4.1 至 4.3	
4.1.1 證書申請實體	4.1 至 4.3	
4.1.2 註冊過程與責任	2.1 及 4.1 至 4.3	
4.2 證書申請處理	4.1 至 4.3	
4.2.1 執行識別與鑒別功能	3.1.8 及 3.1.9	
4.2.2 證書申請批准和拒絕	4.1 至 4.3	
4.2.3 處理證書申請的時間	4. 4	
4.3 證書發出	4.1 至 4.3	
4.3.1 證書發出中註冊機構和電子認證服務機構的行為	4.1 至 4.3	
4.3.2 電子認證服務機構和註冊機構對登記人的通告	4.1 至 4.3	
4.4 證書接受	2.1.4 及 4.1 至 4.3	
4.4.1 構成接受證書的行為	4.1 至 4.3	
4.4.2 電子認證服務機構對證書的發佈	2.5 及 4.1 至 4.3	
4.4.3 電子認證服務機構對其他實體的通告	2.5 及 4.1 至 4.3	
4.5 配對密碼匙和證書的使用	2.1.4 及 2.1.6	
4.5.1 登記人私人密碼匙和證書的使用	2.1.4	
4.5.2 倚據人士公開密碼匙和證書的使用	2.1.6	
4.6 證書續期	3.2	
4.6.1 證書續期的情形	3.2	

RFC3647 的章節	本準則的相關章節	說明
4.6.2 請求證書續期的實體	3.2	
4.6.3 證書續期請求的處理	3.2	
4.6.4 頒發新證書時對登記人的通告	4.1 - 4.3	
4.6.5 構成接受續期證書的行為	4.1 - 4.3	
4.6.6 電子認證服務機構對續期證書的發佈	2.5 及 4.1 至 4.3	
4.6.7 電子認證服務機構對其他實體的通告	2.5 及 4.1 至 4.3	
4.7 證書密碼匙更新	3.2	
4.7.1 證書密碼匙更新的情形	3.2	證書密碼匙將於證書續期過程中被更新
4.7.2 請求證書密碼匙更新的實體	3.2	
4.7.3 證書密碼匙更新請求的處理	3.2	
4.7.4 頒發新證書時對登記人的通告	4.1 - 4.3	
4.7.5 構成接受密碼匙更新證書的行為	4.1 - 4.3	
4.7.6 電子認證服務機構對密碼匙更新證書的發佈	2.5 及 4.1 至 4.3	
4.7.7 電子認證服務機構對其他實體的通告	2.5 及 4.1 至 4.3	
4.8 證書變更	不適用	本準則不接受變更已發出的證書
4.8.1 證書變更的情形		
4.8.2 請求證書變更的實體		
4.8.3 證書變更請求的處理		
4.8.4 頒發新證書時對登記人的通告		
4.8.5 構成接受變更證書的行為		
4.8.6 電子認證服務機構對變更證書的發佈		
4.8.7 電子認證服務機構對其他實體的通告		
4.9 證書撤銷和暫時吊銷	4.5	
4.9.1 證書撤銷的情形	2.1.4, 4.5.1 及 4.10.2	
4.9.2 請求證書撤銷的實體	4.5.2	
4.9.3 撤銷請求的流程	4.5.2	
4.9.4 撤銷請求寬限期	4.5.2	
4.9.5 電子認證服務機構處理撤銷請求的時限	4.5.3	
4.9.6 倚據人士檢查證書撤銷的要求	2.1.6 及 4.5.3	
4.9.7 CRL 發佈頻率	4.5.3 及 4.10.2	
4.9.8 CRL 發佈的最大滯後時間	4.5.3	
4.9.9 在線狀態查詢的可用性	不適用	暫不提供在線狀態查詢服務
4.9.10 在線狀態查詢要求	不適用	暫不提供在線狀態查詢服務
4.9.11 撤銷信息的其他發佈形式	不適用	暫不提供其他發佈形式
4.9.12 密碼匙損害的特別要求	不適用	暫不提供此種服務
4.9.13 證書暫時吊銷的情形	2.1.4 及 4.5.2	
4.9.14 請求暫時吊銷證書的實體	4.5.2	

RFC3647 的章節	本準則的相關章節	說明
4.9.15 請求暫時吊銷的流程	4.5.2	
4.9.16 暫時吊銷的期限限制	4.5.2	
4.10 證書狀態服務	4.5.3 及 4.5.4	
4.10.1 操作特徵	4.5.3	
4.10.2 服務可用性	4.5.3	
4.10.3 可選特徵	4.5.3	
4.11 登記使用期結束	4.6	
4.12 密碼託管與恢復	6.2.3	
4.12.1 密碼匙託管份與恢復的策略與行為	6.2.3	
4.12.2 工作階段密碼匙的封裝與恢復的策略與行為	6.2.3	
5. 認證機構設施、管理和操作控制	2.1.4, 2.1.6, 4 及 5	
5.1 物理控制	5.1	
5.1.1 場地位置與建築	5.1.1	
5.1.2 物理訪問	5.1.2	
5.1.3 電力與空調	5.1.4	
5.1.4 水患防治	5.1.5	
5.1.5 火災防護	5.1.6	
5.1.6 介質存儲	5.1.7	
5.1.7 廢物處理	5.1.10	
5.1.8 異地備份	5.1.8	
5.2 程式控制	5.2	
5.2.1 可信角色	5.2.1	
5.2.2 每項任務需要的人數	5.2.1	
5.2.3 每個角色的識別與鑒別	5.2.1	
5.2.4 需要職責分割的角色	5.2.1	
5.3 人員控制	5.3	
5.3.1 資格、經歷和無過失要求	5.3.1	
5.3.2 背景審查程式	5.3.2	
5.3.3 培訓要求	5.3.3	
5.3.4 再培訓週期和要求	5.3.3	
5.3.5 工作崗位輪換週期和順序	不予以披露	將遵守內部規定，本準則不予以披露
5.3.6 未授權行為的處罰	5.3.4	
5.3.7 獨立合約人的要求	不予以披露	將遵守內部規定，本準則不予以披露
5.3.8 提供給員工的文檔	5.3.5	
5.4 審計日誌程式	4.7	
5.4.1 記錄事件的類型	4.7.1	

RFC3647 的章節	本準則的相關章節	說明
5.4.2 處理日誌的週期	4.7.2	
5.4.3 審計日誌的保存期限	4.7.3	
5.4.4 審計日誌的保護	4.7.4	
5.4.5 審計日誌備份程式	4.7.5	
5.4.6 審計收集系統	4.7.6	
5.4.7 對導致事件實體的通告	4.7.7	
5.4.8 脆弱性評估	4.7.8	
5.5 記錄歸檔	4.8	
5.5.1 歸檔記錄的類型	4.8.1	
5.5.2 歸檔記錄的保存期限	4.8.2	
5.5.3 歸檔文件的保護	4.8.3	
5.5.4 歸檔文件的備份程式	4.8.4	
5.5.5 記錄時間戳要求	4.8.5	
5.5.6 歸檔收集系統	4.8.4	
5.5.7 獲得和檢驗歸檔信息的程式	4.8.4	
5.6 電子認證服務機構密碼匙更替	4.9	
5.7 損害與災難恢復	4.10	
5.7.1 事故和損害處理程序	4.10	
5.7.2 計算資源、軟件和/或數據的損壞	4.10.4	
5.7.3 實體私人密碼匙損害處理常式	4.10.2	
5.7.4 災難後的業務連續性能力	4.10.1	
5.8 電子認證服務機構或註冊機構的終止	4.11 and 4.12	
6. 認證系統技術安全控制	6	
6.1 配對密碼匙的生成和安裝	6.1	
6.1.1 配對密碼匙的生成	6.1.1 及 6.1.5	
6.1.2 私人密碼匙傳送給登記人	6.1.3	
6.1.3 公開密碼匙傳送給證書發出機構	6.1.2	
6.1.4 電子認證服務機構公開密碼匙傳送給倚據人士	4.1 - 4.4	
6.1.5 密碼匙的長度	6.1.4	
6.1.6 公開密碼匙參數的生成和品質檢查	6.1.5	
6.1.7 密碼匙使用目的	6.1.6	
6.2 私人密碼匙保護和密碼模組工程控制	6.2 及 6.7	
6.2.1 密碼模組的標準和控制	6.2.1 及 6.7	
6.2.2 私人密碼匙多人控制（m 選 n）	6.2.2	
6.2.3 私人密碼匙託管	6.2.3	
6.2.4 私人密碼匙備份	6.2.4	
6.2.5 私人密碼匙歸檔	不予以披露	將遵守內部規定，本準則不予以披露

RFC3647 的章節	本準則的相關章節	說明
6.2.6 私人密碼匙於密碼模組之間傳遞	6.2.5	
6.2.7 私人密碼匙在密碼模組的存儲	6.2.5	
6.2.8 啟動私人密碼匙的方法	6.2.4	
6.2.9 解除私人密碼匙啟動狀態的方法	6.2.2	
6.2.10 銷毀私人密碼匙的方法	不予以披露	將遵守內部規定，本準則不予以披露
6.2.11 密碼模組的評估	6.2.1 及 6.7	
6.3 配對密碼匙管理的其他方面	6.3	
6.3.1 公開密碼匙歸檔	6.3	
6.3.2 證書操作期和配對密碼匙使用期限	6.3	
6.4 激活數據	6.1 及 6.2	
6.4.1 激活數據的產生和安裝		
6.4.2 激活數據的保護		
6.4.3 激活數據的其他方面		
6.5 電腦安全控制	6.4	
6.5.1 特別的電腦安全技術要求	6.4	
6.5.2 電腦安全評估	6.4	
6.6 生命週期技術控制	6.5	
6.6.1 系統開發控制	6.5	
6.6.2 安全管理控制	6.5	
6.6.3 生命期的安全控制	6.5	
6.7 網絡的安全控制	6.6	
6.8 時間戳	不適用	暫不提供
7. 證書、憑證撤銷清單和線上證書狀態通訊規約	7	
7.1 證書	7.1	
7.1.1 版本號	附錄 B	
7.1.2 證書擴展項	附錄 B	
7.1.3 演算法物件識別碼	附錄 B	
7.1.4 名稱形式	附錄 B	
7.1.5 名稱限制	附錄 B	
7.1.6 證書策略物件識別碼	附錄 B	
7.1.7 策略限制擴展項的用法	附錄 B	
7.1.8 策略限定詞的語法和語義	附錄 B	
7.1.9 關鍵證書策略擴展項的處理規則	附錄 B	
7.2 證書撤銷清單	7.2	
7.2.1 版本號	附錄 C	
7.2.2 CRL 和 CRL 條目擴展項	附錄 C	
7.3 線上證書狀態通訊規約	不適用	暫不提供

RFC3647 的章節	本準則的相關章節	說明
7.3.1 版本號	不適用	
7.3.2 OCSP 擴展項	不適用	
8. 認證機構審計和其他評估	2.6	
8.1 評估的頻率或情形	2.6	
8.2 評估者的資質	2.6	
8.3 評估者與被評估者之間的關係	2.6	
8.4 評估內容	2.6	
8.5 對問題與不足採取的措施	不予以披露	將遵守內部規定，本準則不予以披露
8.6 評估結果的傳達與發佈	不予以披露	將遵守內部規定，本準則不予以披露
9. 法律責任和其他業務條款	2	
9.1 費用	2.4	
9.1.1 證書發出和更新費用	2.4	
9.1.2 證書查詢費用	2.4	
9.1.3 證書撤銷或狀態資訊的查詢費用	2.4	
9.1.4 其他服務費用	2.4	
9.1.5 退款策略	2.4	
9.2 財務責任	2.2.15	
9.2.1 保險範圍	2.2.15	
9.2.2 其他資產	2.2.15	
9.2.3 對最終實體的保險或擔保	2.2.15	
9.3 業務信息保密	2.7	
9.3.1 保密信息範圍	2.7	
9.3.2 不屬於保密的信息	2.7	
9.3.3 保護保密信息的責任	2.7	
9.4 個人隱私保密	2.7	
9.4.1 隱私保密方案	2.7	
9.4.2 作為隱私處理的信息	2.7	
9.4.3 不被視為隱私的信息	2.7	
9.4.4 保護隱私的責任	2.7	
9.4.5 使用隱私信息的告知與同意	不適用	本準則參照 RFC2527 制定，不披露此部分內容
9.4.6 依法律或行政程式的信息披露	2.7	
9.4.7 其他信息披露情形	2.7	
9.5 知識產權	1.2.2.1	
9.6 陳述與擔保	2	
9.6.1 電子認證服務機構的陳述與擔保	2.2.3	
9.6.2 註冊機構的陳述與擔保	2.1.1	

RFC3647 的章節	本準則的相關章節	說明
9.6.3 登記人的陳述與擔保	2.1.4	
9.6.4 倚據人士的陳述與擔保	2.1.6	
9.6.5 其他參與者的陳述與擔保	不適用	本準則參照 RFC2527 制定，不披露此部分內容
9.7 擔保免責	2.2.10	
9.8 有限責任	2.2.3	
9.9 賠償	2.2.3	
9.10 有效期限與終止	不適用	暫無規定
9.10.1 有效期限		
9.10.2 終止		
9.10.3 效力的終止與保留		
9.11 對參與者的個別通告與溝通	2.1.1	
9.12 修訂	8	
9.12.1 修訂程式	8	
9.12.2 通知機制和期限	8	
9.12.3 必須修改業務規則的情形	8	
9.13 爭議處理	2.3.3	
9.14 管轄法律	2.3.1	
9.15 與適用法律的符合性	2.3.1	
9.16 一般條款	2.3	
9.16.1 完整協議	2.3.2	
9.16.2 轉讓	2.2.5	
9.16.3 分割性	2.3.2	
9.16.4 強制執行	2.3.3	
9.17 其他條款	不適用	本準則參照 RFC2527 制定，不披露此部分內容