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（伺服器）

核證作業準則

日期：2026 年 4 月 16 日
物件識別碼：1.3.6.1.4.1.64092.1.7.1

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中華人民共和國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 G** 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）。

根據本準則，香港互聯網註冊管理有限公司 將稱為香港數碼證書頒發中心。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 F**。

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作為認可核證機關，對其承辦商及核證登記機關在代為執行數碼證書的發出及撤銷等職能或提供相關服務時所作出的行為及活動負責。

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、撤銷及利用公開儲存庫公布已認可及已接受之數碼證書作為在網上進行穩妥的身分辨識。根據本核證作業準則發出的數碼證書（伺服器）為條例下的認可證書，在本核證作業準則內稱為“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。

本核證作業準則符合 RFC3647 互聯網 X.509 公匙基建:證書策略及核證作業架構。

本核證作業之設計旨在符合以下計劃最新版本的要求：

- 核證機關/瀏覽器論壇(CA / Browser Forum) 發佈有關發行和管理公開可信證書的基線要求（ “基線要求” ）；
- 核證機關/瀏覽器論壇發佈有關發行和管理延伸認證證書的準則(“延伸認證 SSL 證書準則”)；
- WebTrust 有關核證機關的原則及準則；
- WebTrust 有關核證機關的原則及準則 – 具網絡安全的 SSL 基線
- WebTrust 有關核證機關的原則及準則 – 延伸認證 SSL

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佈，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佈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》（“業務守則”）相關規例。

香港數碼證書頒發中心已獲 Internet Assigned Numbers Authority (IANA) 分配私人企業號碼 (Private Enterprise Number) 16030 號。**「1.3.6.1.4.1.64092.1.7.1」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）。除了此物件識別碼外，所有符合基線要求的證書亦將包括以下額外識別碼:

SSL 證書	**證書策略物件識別碼 (OID)**
域名認證數碼證書（伺服器）	2.23.140.1.2.1 （由核證機關/瀏覽器論壇分配適用於給符合網域驗證（DV）政策的數碼證書）
機構認證數碼證書（伺服器）	2.23.140.1.2.2 （由核證機關/瀏覽器論壇分配適用於給符合機構驗證（OV）政策的數碼證書）
延伸認證數碼證書（伺服器）	2.23.140.1.1 （由核證機關/瀏覽器論壇分配給符合延伸認證策略的數碼證書）

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。

根據條例，香港數碼證書頒發中心為認可核證機關。**而根據本核證作業準則而發出的數碼證書（伺服器），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、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已指定核證登記機關為其代理人之事實並無減輕香港數碼證書頒發中心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。

本準則符合 RFC 3647 的格式要求。 雖然某些章節標題根據 RFC 3647 的結構包含在本準則中，但該主題不一定適用於香港數碼證書頒發中心的服務， 這些章節會說明為 "没有規定"。標準結構的小節在有需要時會提供額外資訊。符合 RFC 3647 的格式要求增強和利便與其他第三方核證機關的對應和互操作性，並預先為依據人士提供香港數碼證書頒發中心作業實務和程序的通知。

附錄 E 載有根據本準則發出之數碼證書的特點摘要。

1.2 文檔名稱與標識

本文檔為香港數碼證書頒發中心核證機關之核證作業準則，自創建本文檔以來，已進行了下列修訂。

修訂編號	修訂摘要	生效日期
1	首個香港數碼證書頒發中心數碼證書（伺服器）核證作業準則版本。	[TBC]

1.3 公匙基建參與者

1.3.1 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。

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、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。

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、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 2.3 條），
b) 通知申請人有關已批准或被拒絕的申請（見第 4.1 至 4.4 條），
c) 撤銷證書并依時公布證書撤銷清單以及線上證書狀態應答（見第 4.9 條），及
d) 通知登記人有關已撤銷的證書（見第 4.9.5 條）。

1.3.2 註冊機構

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、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。**

參閱**附錄 F** -香港數碼證書頒發中心數碼證書核證登記機關名單（若有的話）

1.3.3 登記人

根據本核證作業準則，登記人指於**附錄 A** 內所指的 “登記人”或 “登記人機構” 。香港數碼證書頒發中心透過其代理人核證登記機關或承辦商發出數碼證書，而核證登記機關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 1.3.2 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。

1.3.3.1 登記人之類別

根據本準則香港數碼證書頒發中心僅發出數碼證書（伺服器）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。

數碼證書（伺服器）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簽發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」），並擬持有以該機構所擁有之一個或多個伺服器名稱發出之證書。數碼證書（伺服器）“通用版” 之伺服器名稱的完整格式網域名稱的最左邊部份可為通配符（即星號 “*” ）。

根據核證機關/瀏覽器論壇指定的物件識別碼（OID），數碼證書（伺服器）分為以下認證類型：

i. 域名認證數碼證書（伺服器）
   - 域名認證數碼證書乃根據核證機關/瀏覽器論壇 “基線要求”的域名驗證規則進行驗證。

ii. 機構認證數碼證書（伺服器）
   - 域名認證數碼證書乃根據核證機關/瀏覽器論壇 “基線要求”的機構驗證規則進行驗證。

iii. 延伸認證數碼證書（伺服器）
   - 證書之驗證程序須根據核證機關/瀏覽器論壇《延伸認證準則》。
   - 延伸認證數碼證書（伺服器）僅支援單一或多個伺服器名稱，但不支援包含通配符之伺服器名稱。

1.3.4 倚據人士

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，倚據人士不應倚據核證登記機關。

1.3.5 其他參與者

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。

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。

參閱**附錄 G** -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）

1.4 證書用途

1.4.1 適當證書用途

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。

數碼證書（伺服器）只可用於加密電子通訊以及伺服器驗證。如證書內之數碼簽署密碼匙使用方法（於**附錄 B** 內指明）有被啟用，此類證書之數碼簽署亦只可用於伺服器驗證以及與伺服器建立安全通訊通道。不論任何情況，此等證書產生之數碼簽署均不得用作洽商或訂定合約或任何具法律效力之協議或任何金錢交易。

1.4.2 限制的證書應用

登記人機構向香港數碼證書頒發中心承諾，不會授權予任何人使用此類證書之數碼簽署作伺服器驗證或與伺服器建立安全通訊通道以外之用途。由此，任何人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。

1.5 策略管理

1.5.1 策略文檔管理機構

本核證作業準則（“準則”）由香港數碼證書頒發中心公布，使公眾有所瞭解，並規定香港數碼證書頒發中心在發出、撤銷及公布數碼證書時採用之做法及標準。

1.5.2 聯繫人

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

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。

1.5.3 確定核證作業準則符合策略的人

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》（“業務守則”）相關規例。

1.5.4 核證作業準則批准程序

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。香港數碼證書頒發中心有權更改此準則而不另行通知（見第 9.12 條）。

1.6 定義和縮寫

參閱附錄 A - 詞彙及縮寫

2. 公布與儲存庫責任

2.1 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簽發並已經由登記人接受的證書清單、最新證書撤銷清單、最新的線上證書狀態應答，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數碼證書有關之其他資料，包括數碼證書申請表及其中包含的《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布及更新儲存庫中有關披露文檔和文檔以往發布、修訂信息的披露記錄。

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。

2.2 認證資料的公布

香港數碼證書頒發中心儲存庫可透過下述 URL 接達：

https://www.hkca.hk
ldap://ldap.hkca.hk

2.3 公佈的時間或頻率

除平均每週兩小時之定期維修及緊急維修外，儲存庫基本保持每日 24 小時、每週 7 日開放。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和線上證書狀態應答等其他相關情況時，儲存庫會盡快作出更新。
香港數碼證書頒發中心每年審查此準則並在必要時對其進行更新。此準則的新版本或修改版通常在其批准後七 (7) 天內發佈。

2.4 儲存庫進入控制

儲存庫所在位置可供在線瀏覽，並可防止擅進。

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。

3. 鑑別及認證

3.1 命名

3.1.1 名稱類型

3.1.1.1 主體名稱

透過證書上的主體名稱（於**附錄 B** 內指明）可識別數碼證書（伺服器）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或香港特別行政區政府各政策局或部門之登記名稱，又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部門或政策局，則為該部門或政策局之正式名稱；及

b) 登記人機構所擁有伺服器（包括伺服器的網域名稱）之名稱。因應香港數碼證書頒發中心的酌情權，伺服器名稱的完整格式網域名稱的最左邊部份可為通配符（即星號“*”），亦即證書可用於登記人機構所擁有的同一域名或子域名的所有伺服器名稱。

如登記人機構申請數碼證書（伺服器）“通用版”或“多域版”，數碼證書（伺服器）將包含主體別名 (Subject Alternative Name)（於**附錄 B** 內指明），其中包括於主體名稱所指由登記人機構擁有的伺服器名稱（包括伺服器的網域名稱）。數碼證書（伺服器）“通用版”之主體別名亦包含一個由登記人機構擁有而不帶有通配符部分的伺服器名稱。至於數碼證書（伺服器）“多域版”之主體別名，則可包含額外的伺服器名稱，而每個額外伺服器名稱必須由該登記人機構擁有。帶有通配符（即星號“*”）的額外伺服器名稱將不會被接受。

3.1.1.2 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（伺服器）之申請手續，然而該證書並不會辨識此獲授權代表身分。

3.1.1.3 機構中文名稱

數碼證書（伺服器）以英文發出，其包含的機構名稱可以是中文或英文。如數碼證書（伺服器）之登記人機構在申請表格內提供中文機構名稱，他們可選擇在數碼證書（伺服器）內顯示中文機構名稱。如機構未有選擇，數碼證書（伺服器）內將顯示其英文機構名稱。對於只有中文機構名稱或只提供中文機構名稱的數碼證書（伺服器）登記人機構，機構的中文名稱將顯示在數碼證書（伺服器）內。

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 登記人的匿名或偽名

香港數碼證書頒發中心不會發出以匿名或假名進行伺服器驗證的證書。

3.1.4 詮釋各個名稱規則

數碼證書（伺服器）會載入之登記人名稱(主體名稱)類型見第 3.1.1 條。有關數碼證書（伺服器）主體名稱之詮釋應參照**附錄 B**。

3.1.5 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。域名的唯一性由網際網路名稱與數字地址分配機構 (ICANN)控制。

3.1.6 商標註冊的認可、認證和角色

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。

香港數碼證書頒發中心可酌情處理有關商標權、服務商標、商用名稱、公司名稱或知識產權之爭議之事宜並享有最終決定權。

3.2 首次身份確認

所有申請人必須透過登記人平台，或（如適用）經承辦商或核證登記機關遞交其數碼證書申請（見附錄 E）。

申請獲批准後，香港數碼證書頒發中心即準備證書並按第 4.3 條所述向申請人發出通知，說明如何發出證書。

對於透過登記人平台遞交的數碼證書申請，香港數碼證書頒發中心將核實（包括但不限於）以下事項：

a) 機構的授權代表已使用「智方便+」在登記人平台建立機構帳戶，並已提供與其香港身份證（HKID）一致的個人身分資料。
b) 授權代表已使用「智方便+」為證書申請進行數碼簽署，而該機構將被視為登記人。

香港數碼證書頒發中心將接受申請人透過「智方便+」所提供的身分認證及數碼簽署作為足夠的身分證明。

對於透過承辦商或核證登記機關遞交的數碼證書申請，香港數碼證書頒發中心會按照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並保留絕對酌情權，在其認為有需要的情況下，要求申請人提供額外資料或文件，以便於個別情況下證明及核實申請人的個人身分。

3.2.1 證明擁有私人密碼匙之方法

申請人在其裝置上自行產生載有其公開密碼匙的「簽發證書要求」（Certificate Signing Request），及將「簽發證書要求」經由香港數碼證書頒發中心位於 https://www.hkca.hk 的指定網頁傳送給香港數碼證書頒發中心。

在收到「簽發證書要求」後，香港數碼證書頒發中心會查證載有公開密碼匙資料的「簽發證書要求」上的數碼簽署，以核對申請人是持有配對的私人密碼匙。香港數碼證書頒發中心並不會持有申請人的私人密碼匙。

3.2.2 組織機構身份的鑒別

在處理機構認證及延伸認證數碼證書（伺服器）的申請時，機構申請人的身份鑒別必須透過以下其中一個運作程序完成。

a) 申請人之獲授權代表須透過數碼證書登記人平台遞交申請，而該申請必須由獲授權代表使用「智方便+」進行數碼簽署。
b) 香港數碼證書頒發中心可酌情容許申請人毋須由獲授權代表親身辦理手續而遞交申請表，惟須符合兩項條件：(1) 申請表須連同獲授權代表已簽署的香港身份證或護照副本；及 (2) 同時符合以下各項要求：
    i. 獲授權代表的身分已於登記人機構以往的申請中獲得認證，並且該獲授權代表曾於該次申請時親身到香港數碼證書頒發中心指定處所，或香港數碼證書頒發中心指定之承辦商或核證登記機關的處所進行身分核實；及
    ii. 有合理理據可再次確認獲授權代表的身分，例如透過與獲授權代表進行電話直接確認，或核對其簽署與以往申請記錄所載的簽署是否一致。
c) 如對獲授權代表的身分真確性有任何懷疑，香港數碼證書頒發中心可酌情拒絕有關申請。

3.2.2.1 數碼證書（伺服器）

每份機構認證數碼證書（伺服器）之申請須附有以下文件供香港數碼證書頒發中心驗證：

a) 蓋上申請機構 “For and on behalf of ”（代表機構簽署）印章及附有該機構申請人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並證明伺服器證書內的主體名稱及主體別名（如有）所載網域名稱擁有權；
b) 由香港特別行政區政府部門或有關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。

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。

3.2.2.2 延伸認證數碼證書（伺服器）

香港數碼證書頒發中心根據核證機關/瀏覽器論壇發佈的延伸認證 SSL 證書準則第 11 條，按照下列各項，核實申請人機構身分的合法存在、實體存在和營運存在：

政府實體或私人機構

a) 如該機構於延伸認證 SSL 證書準則的定義中被視為政府實體或私人機構，每份延伸認證數碼證書（伺服器）的申請必須附有與第 3.2.2.1 條所述相同的文件。對於持有香港特別行政區政府發出的有效商業登記證的私人機構，香港數碼證書頒發中心會依據登記機關和註冊機關發出的有關文件，核實該機構的合法存在。對於屬於法定團體的私人機構，香港數碼證書頒發中心會核實其獲香港特別行政區法例認可的合

法存在，並在有必要時依據註冊機關發出的適用文件進一步核實該機構。

商業實體

b) 如該機構於延伸認證 SSL 證書準則的定義中被視為商業實體，則除了第 3.2.2.1 條所述由登記機關發出的文件外，其獲授權代表須同時遞交由第三方核證人（即香港公證人、執業會計師或執業律師）發出之“專業核證函件”，其中須列明以下附加文件（驗證文件）已由第三方核證人核證：

i) 申請人之個人聲明，包括其個人目前或曾經使用的的全名或名稱（包括所有其他使用過的名稱）、其可供聯絡的居住地址、出生日期，以及確認所有證書內容資料皆為真實且正確無誤之聲明。個人聲明須由申請人簽署，並須與申請表之簽署相同；
ii) 申請人的香港身份證或護照副本；
iii) 至少兩份包括申請人姓名以證明申請人身分的證明文件，其中一份證明文件必須來自金融機構。（1）可接受的金融機構文件包括信用卡/簽帳金融卡（該卡須列出到期日期，且該卡尚未到期）或物業按揭賬單/銀行賬單（發出時間在過去六個月內），及（2）可接受的非金融文件包括能確認固定地址收取服務費用的近期水電煤費賬單正本（不可是移動/手提電話賬單）或租金付款賬單的副本（該證明須列出日期，且日期必須為過去六個月內）；
iv) 商業登記證副本；及
v) 申請人機構之有效的銀行存款賬戶文件副本。

所有上述的驗證文件之正本，必須提供給香港數碼證書頒發中心作核實用途。香港數碼證書頒發中心會與申請人面對面核實及核對以下驗證文件之正本：

i) 核對個人聲明的內容，以確定包括申請人姓名、申請人簽署和居住地址在內的資料與驗證文件正本和申請表中的相對應資料一致；及
ii) 核對驗證文件（包括申請人的香港身份證或護照的副本）是完整、真實和準確複制正本之文件。

香港數碼證書頒發中心在收到“專業核證函件”連同已核對的驗證文件後，香港數碼證書頒發中心會核實第三方核證人是否為香港合法公證人、執業會計師或執業律師，並會確認第三方核證人是否已驗證了該驗證文件。

所有機構認證及延伸認數碼證書（伺服器）申請：

c) 如果申請表中提供的業務地點地址資料無法在相關的香港政府部門或登記機構得到核實時，香港數碼證書頒發中心或承辦商可以實地考察業務地點，以獲取能顯示申請人業務的記錄（例如拍攝固定招牌、業務地點外部、業務地點內部接待區或工作區等照片）。

香港數碼證書頒發中心在有懷疑的情況下，可拒絕有關申請。

3.2.3 個人身份認證

機構申請人的獲授權代表將透過第 3.2.2 條中所述的其中一項運作完成身分認證。

3.2.4 沒有驗證的登記人資料

香港數碼證書頒發中心按照核證機關/瀏覽器論壇基線要求第 7.1.4.2 條中定義的主體名稱和主體別名進行認證。

3.2.5 授權確認

授權確認包含確定獲授權代表是否具有特定權限、權利或許可(包括允許代表登記人機構)以獲得數碼證書 (伺服器)。

所有數碼證書 (伺服器) 的申請，獲授權代表的授權均通過使用核證機關/瀏覽器論壇基線要求第 3.2.2.4 條中列出的一個或多個程序進行驗證，以及根據基線要求第 3.2.5 條的可靠的通訊方法進行。

就延伸認證數碼證書（伺服器）而言，申請人的授權會根據延伸認證 SSL 證書準則第 11.8.3 條作進一步核實。按照該準則第 11.5 條，香港數碼證書頒發中心須發出電郵及獲取申請人回覆，以確認申請表格內提供的電話號碼及電郵地址為核實的通訊方法，並確認透過該電話號碼能可靠地聯絡申請人及驗證獲授權代表獲申請人的授權以代表申請人提交延伸認證數碼證書（伺服器）的申請。

3.2.6 互操作準則

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（伺服器），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。

3.2.7 網域名稱認證

香港數碼證書頒發中心根據第 4.2.1 條的規定驗證申請人對每個完整網域名稱（“FQDN”）的擁有權或控制權。

3.2.8 互聯網規約地址（IP Address）認證

數碼證書（伺服器）證書不支援互聯網規約地址。

3.3 密碼匙更新請求的鑑別及認證

香港數碼證書頒發中心支援在證書期滿前為現有證書提供密碼匙更換以滿足兩個需要：

i) 證書替補，即在申請證書後更改了某些 (或沒有更改) 主體資料，並且登記人希望(或不希望)更換新證書的配對密碼匙;
ii) 證書續期，即登記人希望延長現有證書的使用期限，並更換證書的配對密碼匙。

在以上兩種情況下，必須依據第 4.2.1 條再次確認身份鑑別及認證。

3.3.1 常規密碼匙更新的鑑別及認證

香港數碼證書頒發中心不支援證書常規更換密碼匙以作密碼匙替補的請求。一般證書的密碼匙會於證書續期過程中或因應香港數碼證書頒發中心的酌情權於證書替補過程中被更換。

3.3.2 證書撤銷後密碼匙更新的鑑別及認證

香港數碼證書頒發中心不得為已過期或已撤銷的證書更換密碼匙。

登記人或登記人機構的獲授權代表必須按照第 3.2 條所述的首次登記手續申請證書。

3.4 證書撤銷申請的鑑別及認證

香港數碼證書頒發中心接到登記人或透過代理人提交的首次撤銷證書要求後，會驗證該請求及其原因。經登記人，或經初始接收撤銷證書要求的核證登記機關，最後確認撤銷證書後，該證書即會被撤銷且永久失效。撤銷證書之最後確認程序包括（1）登記人在其提交要求的香港數碼證書頒發中心網站的指定網頁上進行身份認證，（2）收到由登記人以其私人密碼匙進行數碼簽署之電子郵件，（3）登記人親筆簽署之信件正本或（4）登記人親筆簽署之撤銷證書申請表格正本。

4. 證書生命週期操作要求

4.1 證書申請

所有首次申請及證書撤銷或到期後之申請，申請人須依據本核證作業準則第 3 及 4 條指明的程序遞交申請。

4.1.1 誰能遞交證書申請

獲香港特別行政區政府簽發有效商業登記證之申請人其獲授權代表，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，均可向香港數碼證書頒發中心遞交證書申請。

4.1.2 登記過程與責任

數碼證書申請人必須完成登記程序，其中包括:

a) 填妥申請表格並於香港數碼證書頒發中心指定處所或香港數碼證書頒發中心指定的其他機構的處所用遞交；
b) 在登記過程中提供申請表格所規定的證明文件；
c) 繳交所需費用；
d) 產生私人密碼匙及公開密碼匙；
e) 申請人在其裝置上自行產生載有其公開密碼匙的「簽發證書要求」(Certificate Signing Request)，及將「簽發證書要求」經由香港數碼證書頒發中心位於 https://www.hkca.hk 的指定網頁傳送給香港數碼證書頒發中心。

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數碼證書頒發中心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。

4.2 處理證書申請

4.2.1 履行鑑別及認證職能

用以證明登記人機構、獲授權代表身分之文件，於本準則第 3.2.2 條及第 3.2.3 條說明。於成功完成身分核對程序後，一條安全連結將傳送至獲授權代表所指定的電郵地址，以提取密碼。每條安全連結只可使用一次，並會於發出日起一個月後自動失效。同時，香港數碼證書頒發中心會對列於證書上的域名進行核證機關授權記錄之檢查。若核證機關授權記錄存在，但該記錄未有將香港數碼證書頒發中心之域名”hkca.hk”列入為獲授權證書發出者，則其證書申請將不會被繼續處理。若列於證書上的域名並沒有核證機關授權記錄，則香港數碼證書頒發中心認為申請人同意讓香港數碼證書頒發中心為其域名發出證書。

為依循核證機關 / 瀏覽器論壇基線要求 (CA / Browser Forum Baseline Requirements, (BR)) 對確認網域授權的責任要求，香港數碼證書頒發中心確定在發出數碼證書 (伺服器)當日使用以下一個或多個程序以確認申請人對每個列於數碼證書 (伺服器)的完整網域名稱 (Fully-Qualified Domain Name (“FQDN”))之擁有權或控制權:

a) 直接以新組合的電郵地址與域名登記人聯絡以進行核證，新組合電郵地址的區域部份以 ‘admin’, ‘administrator’, ‘webmaster’, ‘hostmaster’ 或 ‘postmaster’ 為開始，跟著是“@”符號，隨後為刪除了零字符或其他字符的申請網域名稱；(即 BR 3.2.2.4.4 所規定) ; 或

b) 確認隨機值是否存在於 1) 申請網域名稱；或 2) 帶有底線字元開頭的網域標籤的申請網域名稱的 DNS CNAME、TXT 或 CAA 的記錄中（即 BR 3.2.2.4.7 所規定）；或

c) 如 FQDN 的基本網域名稱與政府實體相關（例如 example.gov.hk），則驗證申請人（即香港特別行政區政府的局或部門）是否為網域聯絡人（即 BR 3.2.2.4.12 所規定）；或

d) 確認隨機值是否存在於檔案中，而該檔案 1) 位於授權網域名稱（Authorization Domain Name）之中；及 2) 位於「/.well-known/pki-validation」目錄下；及 3) 可透過「http」或「https」協定檢索；及 4) 經由授權通訊埠（Authorized Port）存取（即 BR 3.2.2.4.18 所規定）。

4.2.2 證書申請批准和拒絕

在核對身分手續後，香港數碼證書頒發中心有義務通知申請人其申請已被接納或拒絕。申請被拒絕的申請人隨後可重新申請。香港數碼證書頒發中心有絕對酌情權保留拒絕申請的權力，且無須對因拒絕申請而產生的任何損失或費用承擔任何責任。

4.2.3 處理證書申請的時間

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
域名認證數碼證書（伺服器）	十個工作天
機構認證數碼證書（伺服器）	十個工作天
延伸認證數碼證書（伺服器）	十個工作天

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 4.2.3 條而言，一律不視作工作日計算。

4.3 證書簽發

4.3.1 證書簽發期間核證機關的行為

至少兩名可直接參與證書簽發並且已使用雙重認證登入香港數碼證書頒發中心系統的香港數碼證書頒發中心人員輸入並審核申請人的資料。在成功完成對申請人證書申請所需的核對後，香港數碼證書頒發中心批准其數碼證書 (伺服器) 的申請。

在收到「簽發證書要求」後，香港數碼證書頒發中心會查證載有公開密碼匙資料的「簽發證書要求」上的數碼簽署，以核對申請人是持有配對的私人密碼匙。香港數碼證書頒發中心並不會持有申請人的私人密碼匙。

在核對申請人是持有配對的私人密碼匙後，香港數碼證書頒發中心會產生載有申請人公開密碼匙的數碼證書。為按照 RFC6962 以支持證書透明度(Certificate Transparency)，香港數碼證書頒發中心會將該證書發送到兩個或以上的證書透明度日誌(Certificate Transparency Logs)，以獲取並附加證書簽署時間戳(signed certificate timestamp)於數碼證書上。

4.3.2 核證機關向登記人發出簽發證書通告
在核對身分手續成功後，香港數碼證書頒發中心將發電子郵件到申請人指定的電子郵件地址通知其申請已被接納。

4.4 證書接受

4.4.1 構成接受證書的行為
申請人於香港數碼證書頒發中心指定網頁 https://www.hkca.hk 核對和確認數碼證書的內容是否準確。如申請人拒絕接受數碼證書，香港數碼證書頒發中心會撤銷該數碼證書。當申請人使用數碼證書時，即被視為已接受數碼證書。

申請人可瀏覽證書檔案或經香港數碼證書頒發中心核證機關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。

4.4.2 核證機關對證書的發佈
所有已獲接受並已發出的數碼證書將根據《電子交易條例》的規定在香港數碼證書頒發中心儲存庫公布。

4.4.3 核證機關對其他實體的通告
核證登記機關如有參與發出證書的過程，將可能會收到發出證書的通知。

4.5 配對密碼匙和證書的使用

4.5.1 登記人私人密碼匙和證書的使用
登記人負責：

a) 承認會履行義務，使用合理預防措施來保護其證書私人密碼匙之機密性（即對其保密）及完整性，以防丟失、洩露或未經授權之使用，且須對在任何情況下外洩私人密碼匙而引致的後果負責。
b) 發現其證書的私人密碼匙之任何丟失或外洩時，立即向香港數碼證書頒發中心呈報丟失或外洩（外洩乃屬違反保安，使資料遭受未經授權之進入，從而導致資料有可能在未經授權下被披露、更改或使用）。
c) 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撤銷證書後，均不得在交易中使用證書。
d) 在明知香港數碼證書頒發中心可能據以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，因情形乃屬如此，故倚據人士不得就交易而倚據證書。
e) 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(伺服器)登記人亦負責確保此類證書只可用於加密電子通訊以及伺服器驗證。如證書內之數碼簽署密碼匙使用方法（於**附錄 B** 內指明）有被啟用，不會試圖使用該數碼證書（伺服器）的私人密碼匙以產生數碼簽署並用作伺服器驗證或與伺服器建立安全通訊通道以外之用途。

4.5.2 倚據人士公開密碼匙和證書的使用

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 F**)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或者相關的線上證書狀態應答（如適用）。
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。

4.6 證書續期

4.6.1 證書續期的情形

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（伺服器）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與第 6.3.2 條指明的證書有效期有所不同，最長不超過 199 天：

新證書有效期	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
最多 199 天	新證書產生日期	原有證書（即須續期的證書）到期日之後 199 天或登記期到期日以較早者為準。	新的數碼證書的有效期會有所不同，最長不超過 199 天

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。

4.6.2 誰能要求證書續期

數碼證書（伺服器）不會自動續期。若香港數碼證書頒發中心接收到續期申請，即會根據 3.2.2 條所述“組織機構身份的鑒別”之過程進行認證。機構的獲授權代表須填妥證書續期申請表(可於香港數碼證書頒發中心網址 https://www.hkca.hk 下載)，並連同申請書內列明的其他文件以及續期費用，一併交回。如獲授權代表人選有變，根據第 3.2.2 (a)條中所述，新的獲授權代表亦須填妥申請表，一併交回香港數碼證書頒發中心。

4.6.3 證書續期請求的處理

續期申請規定和程序與首次申請發出證書時的規定和程序大致相同，並將根據第 3.2.2 條所述的 "組織機構身份的鑒別"之過程進行認證。香港數碼證書頒發中心將要求申請人更換其新證書的密碼匙。

4.6.4 發出新證書時對登記人的通告
向申請人發出關於證書續期的通知與本準則第 4.3.2 條中所述有關新數碼證書的方法相同。

4.6.5 構成接受續期證書的行為
申請人構成接受續期數碼證書之行為與本準則第 4.4.1 條中所述相同。

4.6.6 核證機關對續期證書的發佈
香港數碼證書頒發中心發佈續期數碼證書的方式與本準則第 4.4.2 條中描述的方法相同。

4.6.7 核證機關對其他實體的通告
核證登記機關如有參與發出證書的過程，將可能會收到發出證書的通知。

4.7 證書密碼匙更新

4.7.1 證書密碼匙更新的情形
更換證書密碼匙包括在保留相同的主體資料之同時使用新的公開密碼匙和序號產生新證書。一般證書的密碼匙會於證書續期過程中或因應香港數碼證書頒發中心的酌情權於證書替補過程中被更換。

4.7.2 誰能要求證書公開密碼匙更新
香港數碼證書頒發中心只會接受來自同一登記人有關數碼證書更換密碼匙的請求，或酌情處理。但是，香港數碼證書頒發中心不會自動為數碼證書 (伺服器) 續期或要求更換密碼匙。

4.7.3 證書密碼匙更新請求的處理
證書密碼匙更新請求的處理過程與發出新證書程序相同。

4.7.4 發出新證書時對登記人的通告
香港數碼證書頒發中心將通過本準則第 4.3.2 條中所描述的方法通知更新了證書密碼匙的登記人。

4.7.5 構成接受密碼匙更新證書的行為
登記人構成接受密碼匙更新的證書之行為與本準則第 4.4.1 條中列出的相同。

4.7.6 核證機關對密碼匙更新證書的發佈
香港數碼證書頒發中心發佈密碼匙更新證書的方式與本準則第 4.4.2 條中描述的方法相同。

4.7.7 核證機關對其他實體的通告
核證登記機關如有參與發出證書的過程，將可能會收到證書密碼匙更新的通知。

4.8 證書變更
本核證作業準則不允許修改已發出的數碼證書。

4.8.1 證書變更的情形
沒有規定

4.8.2 誰能要求證書變更
沒有規定

4.8.3 證書變更請求的處理
沒有規定

4.8.4 發出新證書時對登記人的通告
沒有規定

4.8.5 構成接受變更證書的行為
沒有規定

4.8.6 核證機關對變更證書的發佈
沒有規定

4.8.7 核證機關對其他實體的通告
沒有規定

4.9 證書撤銷和暫時吊銷
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 5.7.3 條）。

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。暫時吊銷證書不適用於本準則。

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。

4.9.1 證書撤銷的情形
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。

不論何時，若有以下情況，香港數碼證書頒發中心會於 24 小時內按準則中程序撤銷數碼證書（伺服器）：

1) 接到登記人透過香港數碼證書頒發中心指定網頁 https://www.hkca.hk 的數碼證書 (伺服器) 撤銷要求；
2) 接到登記人通知，數碼證書 (伺服器) 的初次申請未經授權，亦沒有給予可追溯之授權；
3) 知道或有理由懷疑登記人的私人密碼匙已外洩；

4) 認為已經證明或證實有方法可以藉著數碼證書中的公開密碼匙輕易計算出登記人的私人密碼匙（例如 Debian weak key，請參閱 https://wiki.debian.org/SSLkeys）；或
5) 知道或有理由懷疑數碼證書 (伺服器) 上之細節不真實或已變得不真實或證書不可靠，包括但不限於不可倚據網域名稱的確認或數碼證書(伺服器) FQDN 的控制權。

不論何時，若有以下情況，香港數碼證書頒發中心可在 24 小時內撤銷數碼證書 (伺服器)，並會在 5 日內按準則中程序撤銷數碼證書 (伺服器)：

6) 接到登記人透過傳真、郵寄信件、電子郵件或親身遞交數碼證書(伺服器) 撤銷要求；
7) 認為數碼證書 (伺服器) 不再符合核證機關/瀏覽器論壇基線要求第 6.1.5 和 6.1.6 條關於密碼匙的大小和公開密碼匙參數生成及品質檢查的要求；
8) 得到證據顯示數碼證書(伺服器) 被不正當使用；
9) 認為登記人未有履行本準則或登記人協議列明之責任；
10) 知道或有理由懷疑數碼證書（伺服器）中的 FQDN 有不合法律許可使用情況（例如法庭或仲裁員已撤銷域名登記人使用網域名稱的權利，域名登記人與申請人之間的相關許可或服務協議已終止，或域名登記人未能續訂網域名稱）；
11) 知道或有理由懷疑數碼證書（伺服器）“通用版” 被使用作核證屬於欺詐誤導的中繼 FQDN；
12) 知道或有理由懷疑數碼證書（伺服器）中的資料有重大變更；
13) 認為數碼證書 (伺服器) 並非根據核證機關/瀏覽器論壇基線要求或本準則妥當發出；
14) 認為、知道或有理由懷疑數碼證書（伺服器）中的任何資料不準確；
15) 香港數碼證書頒發中心根據核證機關/瀏覽器論壇基線要求發出證書的權利屆滿或被撤銷或終止時，有此規定（除非香港數碼證書頒發中心已安排繼續維護撤銷證書清單及/或線上證書狀態應答）；
16) 數碼證書（伺服器）適用之本準則，規例或法例有此規定；
17) 認為登記人未曾繳付登記費；
18) 認為已經證明或證實有方法顯示登記人的私人密碼匙遭受外洩，或者有明確證據顯示用於生成私人密碼匙的特定方法存在缺陷；
19) 知道或有理由相信數碼證書 (伺服器) 中的任何 "主體名稱" 或 "主體別名" (如有的話) 所指明的任何伺服器名稱已不再為登記人機構所擁有；
20) 知道或有理由相信其資料出現在數碼證書（伺服器）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。

現時本準則下的所有中繼證書僅由香港數碼證書頒發中心運作。如果發生以下一種或多種情況，則中繼證書應在七（7）日內被撤銷：

1) 香港數碼證書頒發中心得到證據證明與中繼證書中公開密碼匙相對應的中繼證書私人密碼匙遭受外洩，或不再符合核證機關/瀏覽器論壇基線要求第 6.1.5 和 6.1.6 條關於密碼匙的大小和公開密碼匙參數生成及品質檢查的的要求；
2) 香港數碼證書頒發中心得到證據顯示中繼證書被不正當使用；
3) 香港數碼證書頒發中心確認中繼證書並非根據核證機關/瀏覽器論壇基線要求或本準則發出；
4) 香港數碼證書頒發中心認為中繼證書中的任何資料不正確或誤道；
5) 香港數碼證書頒發中心因任何原因停止核證機關之運作，並且沒有安排另一個核證機關為中繼證書提供撤銷支援;
6) 香港數碼證書頒發中心根據核證機關/瀏覽器論壇基線要求發出證書的權利屆滿或被撤銷或終止時 （除非香港數碼證書頒發中心已安排繼續維護撤銷證書清單及/或線上證書狀態應答）；
7) 根據香港數碼證書頒發中心核證作業準則要求撤銷；或
8) 中繼證書的技術內容或格式給應用軟體供應商或依據人士帶來不可接受的風險。

4.9.2 誰能要求證書撤銷

登記人，或登記人機構的獲授權代表，可透過香港數碼證書頒發中心於 https://www.hkca.hk 的指定網頁、傳真、郵寄信件、電子郵件或親身前往郵局，向香港數碼證書頒發中心提出撤銷證書要求。此外，登記人，依據人士，應用軟體供應商和其他第三方可以提交證書問題報告以通知香港數碼證書頒發中心撤銷數碼證書（伺服器）的合理原因。證書問題報告必須指明要求撤銷的機構，並須指明有證據支持的撤銷原因。香港數碼證書頒發中心可在沒有申請及不作事前通知之情況下撤銷證書。

4.9.3 撤銷請求的程序

香港數碼證書頒發中心收到撤銷證書要求後，將核證該請求並核實撤銷的理由。經登記人，或經初始接收撤銷證書要求的核證登記機關，最後確認撤銷證書後，該證書即會被撤銷且永久失效。撤銷證書之最後確認程序包括（1）登記人在其提交要求的香港數碼證書頒發中心網站的指定網頁上進行身份認證，（2）收到由登記人以其私人密碼匙進行數碼簽署之電子郵件，（3）登記人親筆簽署之信件正本或（4）登記人親筆簽署之撤銷證書申請表格正本。香港數碼證書頒發中心將通過更新證書撤銷清單，或在適用時更新相關的線上證書狀態應答，並按照作業準則程序透過電子郵件（如果有聯繫電子郵件地址）通知登記人撤銷證書（“撤銷通知書”）。如果證書支持線上證書狀態應答，該證書的線上證書狀態應答將在證書到期後保持撤消狀態。撤銷證書申請表格可於網站 https://www.hkca.hk 下載。

香港數碼證書頒發中心核證機關處理以傳真、郵寄信件、電子郵件或親身遞交的撤銷證書要求的辦公時間如下：

星期一至星期五	：	上午九時至下午五時
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。

4.9.4 撤銷請求寬限期

撤銷請求寬限期 ("寬限期") 指登記人必須在其進行撤銷請求的期間。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。

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。

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，或者就作出撤銷證書之決定與更新相關的線上證書狀態應答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。

4.9.5 核證機關處理撤銷請求的時限

在香港數碼證書頒發中心指定的網頁向香港數碼證書頒發中心提交撤銷證書請求，撤銷將在 24 小時內反映在證書撤銷清單中。 對於其他方法的請求，香港數碼證書頒發中心將作出合理努力，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撤銷證書，由下一個工作日開始的 24 小時內，將該撤銷證書資料於證書撤銷清單公布。就所有符合互認證書策略的“互認版”數碼證書而言，處理時間會縮短為一個工作日。然而，證書撤銷清單並不會於各證書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撤銷之狀態。證書撤銷清單每天發布 3 次，並存檔至少 7 年。相反，如證書支援線上證書狀態通訊規約，則證書的線上證書狀態通訊規約應答將立即更新及發佈以反映證書的撤銷狀態。

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 24 小時內，透過電子郵件（如有電子郵件地址）及更新證書撤銷清單和相關的線上證書狀態應答的方式向有關登記人發出撤銷證書通知。

4.9.6 供倚據人士檢查證書撤銷的規定
倚據人士在依據本證書之前，有負責於倚據證書前查核證書撤銷清單上之證書狀態或者相關的線上證書狀態應答。

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。

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撤銷的證書資料時的政策，已列於本準則第 9.6.4 條(倚據人士之義務)及 9.7 條(合理技術及謹慎)。

4.9.7 證書撤銷清單發佈頻率
當電子認證服務機構本身的證書被撤銷時，香港數碼證書頒發中心將及時發布有關信息(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））。

證書撤銷清單及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 https://www.hkca.hk 公布。

4.9.8 發佈證書撤銷清單的最大滯後時間
香港數碼證書頒發中心不採用證書撤銷清單的最大滯後時間。證書撤銷清單通常在產生後的商業合理時間內自動張貼到儲存庫中。

4.9.9 線上撤銷/狀態查詢的可用性
線上證書狀態應答會依據在**附錄 D** 內指明的格式即時更新及公布，以反映證書的撤銷狀態。

4.9.10 線上撤銷查詢規定
倚據人士必須在倚據證書之前，根據第 4.9.6 條確認證書的有效性。

4.9.11 撤銷公告的其他發佈形式
沒有規定

4.9.12 密碼匙資料外洩的特殊規定
任何能提供證書私人密碼匙資料被外洩證據的人士（包括但不限於依據人士及應用軟體供應商），可以透過香港數碼證書頒發中心核證機關網站的密碼匙外洩報告網頁遞交證據，以“密碼匙資料外洩”為理由告知香港數碼證書頒發中心。如果香港數碼證書頒發中心發現或懷疑有私人密碼匙資料被外洩，將以商業合理努力通知登記人，並在發現該等撤銷原因之後或根據本準則第 7.2 條（a）之要求將證書撤銷清單中的撤銷原因代碼更新為“密碼匙資料外洩”。

透過密碼匙外洩報告網頁向香港數碼證書頒發中心遞交的報告包括了密碼匙資料被外洩的證據，其證據的格式必須為以下兩種之一：

a) 以資料被外洩之私人密碼匙簽署並以“香港數碼證書頒發中心的密碼匙資料被外洩證據”為其「通用名稱」的「簽發證書要求」，其簽署可利用存放在香港數碼證書頒發中心儲存庫內之有效證書之公開密碼匙得以核實；或

b) 私人密碼匙本身

4.9.13 證書暫時吊銷的情形
不適用

4.9.14 誰能要求暫時吊銷證書
不適用

4.9.15 要求暫時吊銷的程序
不適用

4.9.16 暫時吊銷的期限限制
不適用

4.10 證書狀態服務

4.10.1 操作特徵
所有被撤銷證書之有關資料（包括表明撤銷證書之原因代碼）將刊載於證書撤銷清單內（見第 7.2 條）。針對支持線上證書狀態通訊規約的證書，其附有原因代碼的證書狀態將包括在個別證書的線上證書狀態應答之中（見第 7.3 條）。

4.10.2 服務可用性
證書狀態服務為 24x7 保持開放。

4.10.3 運作特點
沒有規定

4.11 登記使用期結束
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 5.5.2 條指定之最短之時限。

4.12 密碼匙託管與復原

4.12.1 密碼匙託管與復原的策略與實施
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。

4.12.2 工作階段密碼匙的封裝與復原的策略與實施
沒有規定

5. 設施、管理及運作控制

5.1 實體控制

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 實體訪問
香港數碼證書頒發中心實施商業上具合理實體保安之控制，分為不同的安全區域，並根據不同區域的物理安全要求，採取有效的物理安全控制措施以確保該區域的物理安全。同時，香港數碼證書頒發中心對每一級物理安全層的訪問都必須是可審計和可控的，從而保證每一級物理安全層的訪問都只有獲授權的人員才可以進行。

這些安全控制措施限制了進入就提供香港數碼證書頒發中心核證機關服務而使用之硬件及軟件（包括核證機關伺服器、工作站及任何外部加密硬件模組或受香港數碼證書頒發中心控制之權標），而可使用該等硬件及軟件之人員只限於本準則第 5.2.1 條所述之履行受信職責之人員。在任何時間都對該等進入進行控制及用人手或電子方法監控，以防發生未經授權入侵。門禁系統設有進出時間記錄和超時報警提示，並定期對記錄進行整理歸檔，進出時間記錄將被保留至少 7 年。

5.1.3 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。

5.1.4 水患
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。核證機關亦已制定相應的處理程序以防止水災或漏水對系統造成損害及其它不利後
果。

5.1.5 火災防護
核證機關設施備妥防火計劃及滅火系統。火災防護措施符合香港消防處的要求。機房設置火災自動報警系統和自動滅火系統，設置兩種火災探測器以檢測溫度和煙霧，火災報警系統與滅火系統聯動。

5.1.6 媒體存儲
媒體存儲及處置程序已經開發備妥。

5.1.7 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清除，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。

5.1.8 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 5.7.4 條）

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。

5.2.2 每項任務需要的人數

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。

5.2.3 每個職責的鑑別及認證

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。

5.2.4 需要職責分離的角色

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

5.3 人員控制

5.3.1 資格、經驗和清白要求

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 背景調查程序

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 再培訓週期和要求
香港數碼證書頒發中心及承辦商或其核證登記機關應為其工作人員提供適當和足夠的培訓 (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。

5.3.5 工作崗位輪換週期和順序
沒有規定

5.3.6 未授權行為的處罰
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。

5.3.7 獨立承辦商的要求
被指派履行受信職責的承辦商人員應遵守第 5.3 條定明的職責，並受上述第 5.3.6 條處罰的約束。

5.3.8 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。

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。

5.4 審計日誌程序

5.4.1 記錄事件的類型
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：

核證機關數碼證書和密碼匙生命週期事件，包括：

- 生成、備份、存儲、復原、存檔及銷毀密碼匙；
- 數碼證書的申請、續期和密碼匙更新請求、及撤銷；
- 批准及拒絕數碼證書申請；
- 加密硬件裝置生命週期管理事件；
- 產生證書撤銷清單；
- 簽署線上證書狀態應答；及
- 推出新的證書結構及停用現有的證書結構。

登記人數碼證書生命週期管理事件，包括：

數碼證書申請、續期和密碼匙更新請求、及撤銷；

- 本準則規定的所有驗證行為；
- 批准及拒絕數碼證書申請；
- 數碼證書簽發；
- 產生證書撤銷清單；
- 簽署線上證書狀態應答。

保安事件，包括：

- 成功及不成功到訪公匙基建系統的嘗試；
- 已執行的公匙基建及保安系統行動；
- 保安結構的改變；
- 在數碼證書系統安裝、更新及移除軟件；
- 系統崩潰、硬件故障及其他異常情況；
- 防火牆及路由器的活動；及
- 進出核證機關設施。

記錄必須包括以下成分：

a) 事件的日期及時間；
b) 制作記錄人員的身份；
c) 事件描述。

5.4.2 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。

5.4.3 審核紀錄之存留期間
存檔審核紀錄文檔存留期為十年。

5.4.4 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。

5.4.5 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。

5.4.6 審核收集系統 (內部對外部)
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。

5.4.7 事件主體的通告
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。

5.4.8 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。

5.5 紀錄存檔

5.5.1 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，及線上證書狀態應答
- 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。

5.5.2 存檔保存期限
密碼匙及證書資料以及 5.5.1 中提及之存檔須妥為保存最少十年。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。

5.5.3 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。

5.5.4 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。

5.5.5 電子郵戳要求
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。

5.5.6 存檔收集系統 (內部對外部)
存檔資料由香港數碼證書頒發中心內部收集。

5.5.7 獲取和驗證存檔資料的程序
有關獲取和驗證存檔資料的程序詳情見第 5.5.4 條。

5.6 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 H**）。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 https://www.hkca.hk 公布供大眾取用。原先之根源密碼匙則保留至第 5.5.2 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。

5.7 資料外洩與災難復原

5.7.1 事件和資料外洩處理程序

香港數碼證書頒發中心維護事件處理程序，以指導人員應對安全事件、自然災害以及可能引起系統破壞的類似事件。為了維持證書服務的完整性，香港數碼證書頒發中心定立、匯編和定期測試適當的應急和災害復原計畫和程序。

香港數碼證書頒發中心已制定全面且可行的大規模撤銷事件應對計劃，並每年對計劃進行測試，將測試中獲得的經驗納入計劃，以不斷改進應對能力。

5.7.2 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簽發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爲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。

5.7.3 私人密碼匙資料外洩之程序

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。

如根據本準則簽發數碼證書（伺服器）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。

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簽發數碼證書（伺服器）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。

5.7.4 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。

5.8 核證機關及核證登記機關終止服務

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。

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。

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。

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，其級別至少達到 FIPS 140-2 第 3 級。

就根源證書及中繼證書配對密碼匙，香港數碼證書頒發中心會：

a) 準備並採用密碼匙產生程序，
b) 由合資格的審計人員見證核證機關配對密碼匙之產生過程，或錄製整個核證機關配對密碼匙之產生過程，
c) 由合資格的審計人員提交報告，報告發表意見認為香港數碼證書頒發中心在其密碼匙和數碼證書生成過程中已採用密碼匙產生程序及用於確保配對密碼匙完整性和機密性的控制措施。

6.1.2 私人密碼匙交付予登記人

申請人自行產生私人密碼匙。

6.1.3 公開密碼匙交付予證書發出人

申請人將自行產生公開密碼匙，並須以確保附合以下要求的方式交付香港數碼證書頒發中心：

- 該公開密碼匙在交付過程中不會被更改；及
- 交付者持有與該公開密碼匙配對的私人密碼匙。

6.1.4 核證機關公開密碼匙交付予倚據人士

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。

6.1.5 密碼匙大小

香港數碼證書頒發中心就其根源證書、中繼證書及登記人證書採用以下 RSA 密碼匙長度及雜湊算式。所有證書類別均須符合下列所列的算式及密碼匙長度要求。

證書類別	雜湊算式	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

6.1.6 公開密碼匙參數的生成和品質檢查
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。

6.1.7 密碼匙用途 (按照 X.509 v3 密碼匙使用方法欄位)
數碼證書（伺服器）之密碼匙只可用於加密電子通訊以及伺服器驗證。如數碼證書（伺服器）內之數碼簽署密碼匙使用方法（於**附錄 B** 內指明）有被啟用，數碼證書（伺服器）之數碼簽署只可用於伺服器驗證以及與伺服器建立安全通訊通道。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）只用於簽署(a)證書、(b)證書撤銷清單及(c)線上證書狀態通訊規約簽署人的證書。

6.2 私人密碼匙保護和加密模組控制

6.2.1 加密模組的標準和控制
香港數碼證書頒發中心的加密模組其級別至少達到 FIPS 140-2 第 3 級。

6.2.2 私人密碼匙(m 選 n)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（5 選 3 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 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。

6.2.5 私人密碼匙存檔
所有私人密碼匙均不會存檔。

6.2.6 私人密碼匙於加密模組之間傳遞
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。

6.2.7 私人密碼匙在加密模組的存儲
香港數碼證書頒發中心私人密碼匙在加密模組產生，其級別至少達到 FIPS 140-2 第 3 級。

6.2.8 啟動私人密碼匙的方法
有關啟動私人密碼匙的方法的詳情見第 6.2.2 條。

6.2.9 停用私人密碼匙的方法
有關停用私人密碼匙的方法的詳情見第 6.2.2 條。

6.2.10 銷毀私人密碼匙的方法
香港數碼證書頒發中心之核證機關密碼匙使用期不超過二十五年（見第 5.6 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以及線上證書狀態通訊規約簽署運作程序，均於硬件加密模組內進行。第 5.5 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。

6.2.11 加密模組的評估
有關加密模組分級的詳情見本準則第 6.2.1 條。

6.3 配對密碼匙管理其他範疇

6.3.1 公開密碼匙存檔
密碼匙及證書資料以及第 5.5.1 條提及之存檔紀錄均妥為保存最少七年。

香港數碼證書頒發中心之核證機關密碼匙使用期不超過二十五年（見第 5.6 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以及線上證書狀態通訊規約簽署運作程序，均於硬件加密模組內進行。第 5.5 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。

6.3.2 證書運作期限和配對密碼匙使用期限
香港數碼證書頒發中心之核證機關密碼匙使用期不超過二十五年（見第 5.6 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以及線上證書狀態通訊規約簽署運作程序，均於硬件加密模組內進行。第 5.5 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。

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。

根據本準則向新申請人發出的證書，其有效期為 199 日。

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不同於上述之有效期(見第 4.6 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**。

6.4 啟動數據

6.4.1 啟動數據的產生和安裝
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。

6.4.2 啟動數據的保護
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（5 選 3 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。

6.4.3 啟動數據的其他方面
沒有規定

6.5 電腦保安控制

6.5.1 特定電腦保安技術要求
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關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 8 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，清除所有可能影響認證業務安全性的信息存儲並加以確認。

6.5.2 電腦保安評估
沒有規定

6.6 生命週期技術控制

6.6.1 系統開發控制
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關人員或在特殊情況下由其它機關進行開發工作，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。

6.6.2 保安管理控制
香港數碼證書頒發中心透過程序實施對其核證機關系統的保安相關配置和保安軟體更改的控制。這些程序包括檢查應用程式和保安軟體的完整性。

6.6.3 生命週期的保安控制
沒有規定

6.7 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關網絡環境的安全，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。

香港數碼證書頒發中心至少每季進行一次漏洞掃描，並至少每年進行一次滲透測試。所有已識別的漏洞會被即時修復，通常在保安修補程式發布後一個月內完成。香港數碼證書頒發中心會進行風險評估，以決定適當的漏洞緩解策略及時間表，並妥善記錄評估結果。如未能於一個月內完成修復，香港數碼證書頒發中心會評估相關風險，並制定及執行有記錄的緩解計劃。

6.8 電子郵戳

香港數碼證書頒發中心使用網路時間協定 (NTP) 與可靠的時間服務至少每八小時一次同步更新其電腦上的系統時間(Windows 預設)。香港數碼證書頒發中心不向公眾提供任何電子郵戳服務。

7. 證書、證書撤銷清單及線上證書狀態應答結構

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）。**附錄 E** 載有數碼證書（伺服器）之特點摘要。

香港數碼證書頒發中心核證機關系統會透過密碼學安全偽亂數生成器（CSPRNG）產生包含至少 64 位元並且大於零 (0) 的非連續數碼證書序號。

7.1.1 版本編號

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**）。

7.1.2 證書延伸欄位

本準則提及之證書格式詳情見**附錄 B**。

7.1.3 算式物件識別碼

本準則提及之證書格式詳情見**附錄 B**。

7.1.4 名稱格式

本準則提及之證書格式詳情見**附錄 B**。

7.1.5 名稱限制

本準則提及之證書格式詳情見**附錄 B**。

7.1.6 證書策略物件識別碼

本準則提及之證書格式詳情見**附錄 B**。

7.1.7 策略限制延伸欄位使用的政策

本準則提及之證書格式詳情見**附錄 B**。

7.1.8 策略限定資格的語法和語義的政策

本準則提及之證書格式詳情見**附錄 B**。

7.1.9 關鍵證書策略延伸欄位的語義處理

本準則提及之證書格式詳情見**附錄 B**。

7.2 證書撤銷清單結構

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撤銷的數碼證書的資訊。

當數碼證書（伺服器）因以下其中一個原因被撤銷時，證書對應的證書撤銷清單的撤銷原因代碼延伸欄位必須包含指定的撤銷理由識別碼。當撤銷理由識別碼不是以下其中一個時，證書撤銷原因代碼延伸欄位將不會提供撤銷理由識別碼：

撤銷原因	撤銷理由識別碼 (RFC5280 中指明的證書撤銷清單原因 (CRLReason))
密碼匙資料外洩	1 = 密碼匙資料外洩 (keyCompromise)
特權被撤銷	9 = 特權被撤銷 (privilegeWithdrawn) (撤銷理由識別碼“特權被撤銷”不需要作為撤銷原因選項提供給證書登記人，因使用該撤銷理由識別碼是由核證機關操作員決定而不是登記人。)
終止營運	5 = 終止營運 (cessationOfOperation)
聯繫變更	3 = 聯繫變更 (affiliationChanged)
證書被取代	4 = 證書被取代 (superseded)

以下說明香港數碼證書頒發中心核證機關或登記人有義務使用撤銷理由識別碼的各個撤銷情況：

a) 撤銷理由識別碼（1）“密碼匙資料外洩”

當發生以下一個或多個情況時，將會使用撤銷理由識別碼“密碼匙資料外洩”：

- 香港數碼證書頒發中心核證機關得到可核實的證據，證明與證書中公開密碼匙相對應的證書登記人私人密碼匙遭受外洩；或
- 香港數碼證書頒發中心核證機關得知已經證明或證實有方法顯示證書登記人的私人密碼匙遭受外洩；或
- 有明確證據顯示用於生成私人密碼匙的特定方法存在缺陷；或
- 香港數碼證書頒發中心核證機關得知一種已經證明或證實有方法，該方法可以藉著證書中的公開密碼匙輕易計算出證書登記人的私人密碼匙（例如 Debian weak key，請參閱 https://wiki.debian.org/SSLkeys）；或
- 證書登記人要求香港數碼證書頒發中心核證機關以此撤銷理由撤銷證書，撤銷範圍說明如下。

如要求以“密碼匙資料外洩” 理由撤銷證書的任何人士，透過本準則第 4.9.12 條所述的香港數碼證書頒發中心核證機關網站上的密碼匙外洩報告網頁證明其以往或目前擁有證書的私人密碼匙，則香港數碼證書頒發中心核證機關將撤銷涵蓋所有登記人有出現該密碼匙的所有情況。

如證書登記人以“密碼匙資料外洩” 理由要求香港數碼證書頒發中心核證機關撤銷證書，並且沒有證明其以往或目前擁有證書的相關私人密碼匙，香港數碼證書頒發中心核證機關可以撤銷與該登記人相關的所有包含該公開密碼匙的證書。

當香港數碼證書頒發中心核證機關得到可核實的證據證明證書私人密碼匙外洩，但證書撤銷清單資料並不包含原因代碼延伸欄位，或包含非“密碼匙資料外洩”理由於原因代碼延伸欄位時，則香港數碼證書頒發中心核證機關可以更改證書撤銷清單將“密碼匙資料外洩”理由作為撤銷理由識別碼加入原因代碼延伸欄位。此外，當香港數碼證書頒發中心核證機關確定證書的私人密碼匙在證書撤銷清單中指示的撤銷日期之前已被外洩時，可以更改該證書在證書撤銷清單中的撤銷日期。

（注意：根據 RFC 5280 第 5.3.2 條中描述，將撤銷日期追溯至過去某時是最佳做法的

一個例外情況；但是，本準則為支援應用軟體供應商，會使用證書首次外洩日期作為撤銷日期。）

否則，不得使用“密碼匙資料外洩”撤銷理由識別碼。

b) 撤銷理由識別碼（9）“特權被撤銷”

撤銷理由識別碼“特權被撤銷”旨在用於登記人涉及未導致“密碼匙資料外洩”的違規行為的情況，例如證書登記人在其證書申請中提供了誤導性信息，或登記人未堅守其在登記人協議或使用條款之重大義務。

除非 “密碼匙資料外洩”撤銷理由識別碼已被使用，否則在以下情況下必須使用撤銷理由識別碼“特權被撤銷”：

- 香港數碼證書頒發中心核證機關得到證書被不正當使用的證據；或
- 香港數碼證書頒發中心核證機關得知證書登記人違反了登記人協議或使用條款中的一個或多個重大義務；或
- 香港數碼證書頒發中心核證機關得知數碼證書（伺服器）” 通用版” 證書被使用作核證屬於欺詐誤導的中繼完整網域名稱(FQDN)；或
- 香港數碼證書頒發中心核證機關得知證書中的所載資料有重大變動；或
- 香港數碼證書頒發中心核證機關確定或得知證書中的任何資料不準確；或
- 香港數碼證書頒發中心核證機關得知證書的初次申請未經授權，且登記人亦沒有給予可追溯之授權。

否則，不得使用“特權被撤銷”撤銷理由識別碼。

c) 撤銷理由識別碼（5）“終止營運”

撤銷理由識別碼“終止營運”旨在用於使用證書的網頁在證書到期前關閉的情況，或登記人不再擁有或控制證書中指明的網域名稱。此撤銷理由識別碼旨在以下情況使用：

- 證書登記人不再控制或不再被授權使用證書中指明的所有網域名稱；或
- 證書登記人因為將終止其網站而不再使用證書；或
- 香港數碼證書頒發中心核證機關得知任何情況表明使用在證書中的完整網域名稱(FQDN)不再合法（例如法庭或仲裁員已撤銷域名登記人使用網域名稱的權利，域名登記人與申請人之間的相關許可或服務協議已終止，或域名登記人未能續訂網域名稱）。

除非 “密碼匙資料外洩”撤銷理由識別碼已被使用，否則在以下情況下必須使用撤銷理由識別碼“終止營運”：

- 證書登記人已為此原因要求撤銷其證書；或
- 香港數碼證書頒發中心核證機關收到可核實的證據，證明證書登記人不再控制或不再被授權使用證書中指明的所有網域名稱。

否則，不得使用“終止營運”撤銷理由識別碼。

d) 撤銷理由識別碼（3）“聯繫變更”

撤銷理由識別碼“聯繫變更”旨在用於表明證書中的主體名稱或其他主體識別資料已更改，但沒有理由懷疑證書的私人密碼匙已被外洩。

除非 “密碼匙資料外洩”撤銷理由識別碼已被使用，否則在以下情況下必須使用撤銷理由識別碼“聯繫變更”：

- 證書登記人已為此原因要求撤銷其證書；或
- 香港數碼證書頒發中心核證機關因證書的主體資料轉變而重新發出證書，而且核證機關並沒有用其他撤銷證書原因（包括“密碼匙資料外洩”、“證書被取代”、“終止營運”或“特權被撤銷”）更換此證書。

否則，不得使用“聯繫變更”撤銷理由識別碼。

e) 撤銷理由識別碼（4）“證書被取代”

撤銷理由識別碼“證書被取代”旨在用於顯示以下情況：

- 證書登記人已要求以新證書替換現有證書；或
- 香港數碼證書頒發中心核證機關得到合理證據，證明不可倚據網域名稱的確認或證書之完整網域名稱(FQDN)的控制權；或
- 香港數碼證書頒發中心核證機關基於要遵守守則的原因撤銷證書，例如證書不符合本準則、核證機關/瀏覽器論壇(CA/Browser Forum)的基線要求或主要的根源證書計劃的核證政策（例如 Mozilla 根源證書存儲政策）。

除非 “密碼匙資料外洩”撤銷理由識別碼已被使用，否則在以下情況下必須使用撤銷理由識別碼“證書被取代”：

- 證書登記人已為此原因要求撤銷其證書；或
- 香港數碼證書頒發中心核證機關因域名授權或遵守守則出現問題（而不是與“密碼匙資料外洩”或“特權被撤銷”相關的問題）而撤銷證書。

否則，不得使用“證書被取代”撤銷理由識別碼。

有關證書撤銷清單結構詳情見**附錄 C**。

7.2.1 版本編號

香港數碼證書頒發中心之證書撤銷清單一律以 X.509 第二版本之格式發出（見**附錄 C**）。

7.2.2 證書撤銷清單及證書撤銷清單資料延伸欄位

證書撤銷清單及證書撤銷清單資料延伸詳情見**附錄 C**。

7.3 線上證書狀態應答結構

通過發佈一個包含以下主體名稱的線上證書狀態通訊規約簽署人證書，香港數碼證書頒發中心已授權一個線上證書狀態通訊規約應答伺服器為根源證書 CA 及中繼證書進行線上證書狀態通訊規約的簽署。

根源證書：

證書主體名稱 (CN)	線上證書狀態通訊規約簽署人證書主體名稱 (CN)
“HKCA Root CA 2”	“HKCA Root CA 2 OCSP Responder”

中繼證書：

證書主體名稱 (CN)	線上證書狀態通訊規約簽署人證書主體名稱 (CN)
“HKCA d-Cert DV SSL CA 2 - 25”	“HKCA d-Cert DV SSL CA 2 - 25 OCSP Responder”
“HKCA d-Cert OV SSL CA 2 - 25”	“HKCA d-Cert OV SSL CA 2 – 25 OCSP Responder”
“HKCA d-Cert EV SSL CA 2 - 25”	“HKCA d-Cert EV SSL CA 2 - 25 OCSP Responder”

有關線上證書狀態應答結構詳情見**附錄 D**。

7.3.1 版本編號

香港數碼證書頒發中心線上證書狀態應答符合 RFC6960 和 RFC5019（見**附錄 D**）。

7.3.2 線上證書狀態應答延伸欄位

線上證書狀態應答延伸欄位詳情見**附錄 D**。

8. 遵守規定審核和其他評估

本準則中的實務守則旨在滿足或超過行業標準 (如 WebTrust 對核證機關) 的要求。香港數碼證書頒發中心作為認可核證機關，須根據條例 43 (1)編寫和提交評估報告。

8.1 評估的頻率及情形

遵守規定審核及評估須至少每 12 個月進行一次。

8.2 評估者的資格

需聘請符合條例及認可核證機關業務守則規定資格的之獨立外部審計人員進行遵守規定評估。WebTrust 審計員必須符合核證機關/瀏覽器論壇基線要求第 8.2 條的要求。

8.3 評估者與被評估實體之間的關係

根據條例及認可核證機關業務守則所規定，香港數碼證書頒發中心須聘請與之不相關之獨立外部審計人員進行遵守規定評估。

8.4 評估內容

須根據條例以及認可核證機關業務守則之規定進行遵守規定之評估，檢視香港數碼證書頒發中心發出、撤銷及公布證書之系統是否妥善遵守本準則。

8.5 對問題與不足採取的措施

如審核報告指出有任何不符合法律、本準則或任何其他與香港數碼證書頒發中心服務相關之其他構成合約之義務，則 (1) 審計人員將記錄其差異，(2) 審計員將人及時通知香港數碼證書頒發中心，(3) 視差異的性質和程度，香港數碼證書頒發中心將制定一個適當的修正行動計畫以消除不符合的地方，並決定是否對已經發出的數碼證書採取任何補救行動。

8.6 評估結果的傳達與發佈

核證機關的 WebTrust 審核報告在 https://www.hkca.hk/cps 提供給公眾。根據條例 43 (1) 條所訂的遵守規定評估報告，則會呈交數字政策專員。

8.7 自我評估

香港數碼證書頒發中心至少每季度對自上次自我審計以後發佈的數碼證書中隨機選擇至少 3%的樣本進行自我審核。數碼證書的自我審核須按照核證機關/瀏覽器論壇通過的準則進行。

9. 法律責任和其他業務條款

9.1 費用

香港數碼證書頒發中心可不時釐定其處理新申請及續期申請、撤銷要求、行政事宜及任何其他與數碼證書相關服務之收費。現行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權利可不時更改此收費表，並可透過其他方式公布。

除非獲香港數碼證書頒發中心豁免，所有適用費用均須由數碼證書登記人在每一個登記期開始前（見第 3.2 節）繳付全數。若其登記於證書所指明的有效期內終止，香港數碼證書頒發中心可暫停或撤銷該數碼證書（另見第 4.5.1.4(f) 節）。

在一年登記期內，登記人可在同一申請下無限次獲取新證書，而無須另行收費。新證書的有效期會以各階段的最長有效期或剩餘登記期中較短者為準。

9.2 財務責任

9.2.1 保險範圍

香港數碼證書頒發中心維持一般商業責任保險涵蓋至少 200 萬美元，及延伸認證 SSL 證書準則中規定的職業責任/過失保險至少 500 萬美元。此外，另一獨立之保單已經備妥，有關證書之潛在或實質責任以及根據電子交易條例的規定對倚據限額之索償均獲承保。

9.2.2 其他資產

沒有規定

9.2.3 對最終實體的保險或擔保

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。

9.3 業務資料機密

9.3.1 機密資料範圍

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；香港數碼證書頒發中心或承辦商需根據本準則履行其責任之情況除外。

9.3.2 不屬於機密的資料

任何未列為機密的資訊都被視為公共資訊。已發佈的證書和撤銷資料被視為公共資訊。

9.3.3 保護機密資料的責任

在履行與香港數碼證書頒發中心發出、撤銷及公布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、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此條限制事項。

除非經法庭發出之傳召或命令要求，或香港法例另有規定，否則未經登記人事先同意，不得將該等資料對外發布。除非法庭發出傳票或命令，或香港法例另有規定，香港數碼證書頒發中心尤其不得發表登記人清單或其資料，惟無法追溯個別人登記人之綜合資料除外。

9.4 個人資料隱私

9.4.1 隱私方案
香港數碼證書頒發中心實施了一項符合本準則的隱私政策。香港數碼證書頒發中心隱私政策在香港數碼證書頒發中心網站 https://www.hkca.hk 發佈。

9.4.2 視作隱私的資料
任何不在已發出的證書、儲存庫和證書撤銷清單公開的登記人資料均視作隱私資料。

9.4.3 不被視作隱私的資料
已發佈的證書及撤銷資料均被視作公開資料。證書狀態資訊和任何證書內容均視作非隱私資料。

9.4.4 保護隱私的責任
在履行與香港數碼證書頒發中心發出、撤銷及公布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、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此條限制事項。

9.4.5 使用隱私資料的通告與同意
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；香港數碼證書頒發中心或承辦商需根據本準則履行其責任之情況除外。

9.4.6 依法律或行政程序的資料披露
除非經法庭發出之傳召或命令要求，或香港法例另有規定，否則未經登記人事先同意，不得將該等資料對外發布。除非法庭發出傳票或命令，或香港法例另有規定，香港數碼證書頒發中心尤其不得發表登記人清單或其資料，惟無法追溯個別人登記人之綜合資料除外。

9.4.7 其他資料披露情形
沒有規定

9.5 知識產權
香港數碼證書頒發中心擁有與其資料庫、網站、數碼證書、商標和來自香港數碼證書頒發中心的任何其他出版物 (包括本準則) 相關的所有知識產權。

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。

9.6 陳述與擔保

9.6.1 核證機關的陳述與擔保

認可證書一經登記人接受及發出後，香港數碼證書頒發中心發佈在其儲存庫中 (見第 2 條)。

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 9.6.4 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 9.6.4 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。

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署、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。

9.6.2 核證登記機關的陳述與擔保

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、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。**

9.6.3 登記人的陳述與擔保

各申請人（申請數碼證書（伺服器），獲授權代表會代表申請人）須簽署或確定接受一份協議（按本準則規定之條款），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（伺服器）登記人的授權用戶外，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（伺服器）將只會用於第 1.4 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。

登記人負責：

a) 適當完成申請程序並在適當表格內簽署或確定接受登記人協議(由獲授權代表完成)；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。
b) 準確地按照本準則所載關於證書之程序直至證書過期。
c) 不時將登記人提供之證書資料或授權用戶之任何變動立即通知香港數碼證書頒發中心。
d) 將可能致使香港數碼證書頒發中心根據下文第 4 條所載之理由行使權利，撤銷由該登記人負責之證書之任何事項立即通知予香港數碼證書頒發中心。
e) 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撤銷證書後，均不得在交易中使用證書。
f) 在明知香港數碼證書頒發中心可能據以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，因情形乃屬如此，故倚據人士不得就交易而倚據證書。
g) 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。
h) 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。

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。

9.6.4 倚據人士的陳述與擔保

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 F**)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或者相關的線上證書狀態應答(如適用)。
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。

9.6.5 其他參與者的陳述與擔保

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。

9.7 擔保免責

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、郵政署、及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（郵政署、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。

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。

9.8 有限責任

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。

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。**

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任何情況下每份機構認證數碼證書（伺服器）或延伸認證不得超過 20 萬港元，或每份域名認證數碼證書（伺服器）最多 0（零）港元。

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、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。

無論香港數碼證書頒發中心署、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署、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署及上述機構及個人免受此等法律行動。

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。

9.9 賠償

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署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（經香港數碼證書頒發中心署、承辦商，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或者相關的線上證書狀態應答（如適用）；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、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依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，向每名依據證書人士支付最多港幣 200,000 元；如本證書為域名認證數碼證書（伺服器），則支付最多港幣 0（零）元。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港幣 200,000 元，或港幣 0（零）元（如本證書為域名認證數碼證書（伺服器）），而在所有情形下，就第 (1) 及 (2) 類損失而言倚據限額則為港幣 0（零）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、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沒有規定於個人傷害或死亡之(不大可能發生之)情形。”

9.10 有效期限與終止

9.10.1 有效期限

有關準則一經香港數碼證書頒發中心在網頁 https://www.hkca.hk/cps 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。

9.10.2 終止

本準則 (包括所有修訂和增編) 繼續有效，直到被更新版本取代為止。

9.10.3 終止與保留效力

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。

9.11 參與人士的個別通告與通知

若本準則之任何條款被宣布或認為非法、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。

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

9.12 修訂

9.12.1 修訂程序

香港數碼證書頒發中心批准更新其核證作業準則後，有關準則一經香港數碼證書頒發中心在網頁 https://www.hkca.hk 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。

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。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。

9.12.2 通知機制和期限

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 https://www.hkca.hk 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。

9.12.3 必須修改物件識別碼的情形

香港數碼證書頒發中心有權決定核證作業準則的修訂是否需要同時更改物件識別碼(OID)。

9.13 爭議處理

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

9.14 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。

9.15 適用法律的符合性

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。

9.16 一般條款

9.16.1 完整協議

本準則中英文本措詞詮釋若有歧異，以英文本為準。

9.16.2 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。

9.16.3 分割性

若本準則之任何條款被宣布或認為非法、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。

9.16.4 執行 (律師費和放棄權利)

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

9.16.5 不可抗力

如果香港數碼證書頒發中心由於以下原因被阻止、被禁止或者延遲履行或無法履行任何行爲或要求，香港數碼證書頒發中心將不承擔責任：由於任何適用的法律、條例或者命令之規定；由於任何民政當局或軍事當局；斷電、通信中斷或由任何香港數碼證書頒發中心無法控制之人士提供之其他系統失效；火災、洪水或其他緊急狀態；罷工，恐怖襲擊或戰爭；不可抗力；或者其他類似超出香港數碼證書頒發中心合理控製並且非因其無疏忽過錯而造成之情形。

9.17 其他條款

9.17.1 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 9.8 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。

附錄 A - 詞彙及縮寫

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。

“應用軟體供應商”指互聯網瀏覽器軟件或其他依據人士應用軟件的供應商，該軟件顯示或使用證書並包含香港數碼證書頒發中心根源證書。

“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布無效之公開密碼匙中繼證書之資料。

“商業實體”指任何根據延伸認證 SSL 證書準則定義的非私人機構、非政府實體及非商貿實體之登記人機構，登記人機構並非有限公司且僅持有香港特別行政區政府稅務局發出的商業登記證 (BR)。

“核證機關/ 瀏覽器論壇基線要求” 指核證機關/瀏覽器論壇(CA / Browser Forum)在 https://cabforum.org 中發佈，有關發行和管理公開可信證書的基線要求。

“核證機關授權記錄”指一種核證機關授權域名系統資源記錄，使得域名擁有者可以指定認可的核證機關為該域名發出證書。

“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。

“核證機關”指向他人(可以為另一核證機關)發出證書者。

“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。

“證書問題報告”指對涉嫌密碼匙洩露，證書濫用或其他類型的欺詐，妥協，濫用或與證書相關的不當行為的投訴。

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

“證書透明度”指按照 RFC6962 和 Google 的要求，所提供給公開審核及監視的一個有關核證機關發出數碼證書的日誌。

“證書透明度日誌”是一個加密的、可公開審核的、僅限附加記錄伺服器數碼證書的一個簡單的網絡服務。

“密碼匙外洩報告網頁”是香港數碼證書頒發中心核證機關網站上的一個網頁，用於向香港數碼證書頒發中心報告與證書相關的懷疑私人密碼匙資料外洩。

“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 G**，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。

“網域名稱”表示網域名稱系統中分配的節點標籤。

“域名登記人”指對域名有控制使用權的個人或機構。

“域名註冊機構”指負責域名註冊的個人或機構，支持或參與以下協定: (i) 網際網路名稱與數字地址分配機構 (ICANN)，(ii) 國家域名管理/註冊局，或 (iii) 網路資訊中心（包括其分支機搆、 承辦商、 代表、 繼任者或委託人）。

“域名認證”就支援域名認證的香港數碼證書頒發中心數碼證書（伺服器）而言，是指一種證書，其主體資料內容符合核證機關／瀏覽器論壇基線要求中對域名認證證書所指明的資料規定，並且其申請人對有關域名之控制權已按照核證機關／瀏覽器論壇基線要求獲得認證。

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

“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。

“延伸認證”就支援延伸認證的香港數碼證書頒發中心數碼證書（伺服器）而言，是指包含延伸認證 SSL 證書準則中指定的主體資料，並已根據延伸認證 SSL 證書準則進行認證的數碼證書。

“延伸認證 SSL 證書準則”指核證機關/瀏覽器論壇在 http://www.cabforum.org 發佈有關發行和管理延伸認證證書的準則。

“完整網域名稱”指包含網域名稱系統中所有上級節點標籤的網域名稱。

“政府實體”根據核證機關/瀏覽器論壇的“延伸認證 SSL 證書準則”定義而言，指香港特別行政區政府政策局或部門。

“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。

“香港”指中華人民共和國香港特別行政區。

“註冊機關”就延伸認證數碼證書（伺服器）而言：

(a) 在“私人機構”的文意下，指香港特別行政區政府公司註冊處（見 https://www.cr.gov.hk/），在其職能下登記該實實體的合法存在；或

(b) 在“政府實體”的文意下，指制定香港特別行政區法例、規例或判令以成立政府實體合法存在的實體。

“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。

“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。

“多域版”就一張數碼證書（伺服器）而言，指在證書主體別名內列出額外伺服器名稱，使證書可用於多個伺服器名稱之特點。

“公證人”指持有有效公證人委任證明書並在香港特別行政區高等法院備存的公證人註冊紀錄冊上註冊之律師。

“OCSP”指線上證書狀態通訊規約。

“線上證書狀態通訊規約”指一種線上證書核對規約，允許倚據人士查明數碼證書的狀態。

“條例”指香港法例第 553 章《電子交易條例》。

“機構認證”就支援機構認證的香港數碼證書頒發中心數碼證書（伺服器）而言，指一種證書，其主體資料內容符合核證機關／瀏覽器論壇基線要求中對機構認證證書所指明的資料規定，並且其申請人的機構身分及域名擁有權已按照核證機關／瀏覽器論壇基線要求獲得認證。

“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。

“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。

“執業會計師”指持有根據《專業會計師條例》（第 50 章）發出有效執業證書的會計師。

“執業律師”指持有有效執業證書並在香港特別行政區高等法院備存的律師登記冊上登記的律師。

“私人密碼匙”指配對密碼匙中用作產生數碼簽署之密碼匙。

“私人機構” 根據核證機關/瀏覽器論壇的“延伸認證 SSL 證書準則”定義而言，指任何持有公司註冊處簽發的公司註冊證書 (CI) 及香港特別行政區政府稅務局簽發的商業登記證 (BR）的登記人機構，或獲香港特別行政區法律認可之本港法定團體。

“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第 21 條認可之核證機關或第 34 條所述核證機關。

“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。

“登記機關”指為組建業務或根據許可證、契約或其他證明授權開展業務的實體進行登記商業資訊的香港特別行政區政府稅務局（見 https://www.ird.gov.hk/）。

“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。

“可靠的通訊方法”指除由獲授權代表提供以外的已核實通訊方法，如郵寄快遞地址、電話號碼或電郵地址。

“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。

“證書簽署時間戳”指當提交一張有效的伺服器數碼證書到一個證書透明度日誌後，該日誌會發出一個證書簽署時間戳，以表示容許將該證書在某特定時間內加到日誌內。

“智能身份證”指可將數碼證書載入其中的身份證。

“S/MIME”即保密／多功能互聯網郵遞伸延的縮寫。

“SSL”即保密插口層的縮寫。

“中繼證書”指由香港數碼證書頒發中心的根源證書所簽發的中繼核證機關證書，並用於簽發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。

“主體名稱”指證書持有者名字的信息。

“TLS”即傳輸層保安協定的縮寫。

“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。

“專業核證函件”指根據核證機關／瀏覽器論壇延伸認證 SSL 證書準則中規定之已核實的會計師函件或已核實的法律意見書。

“WebTrust for Certification Authorities” 即在 http://www.webtrust.org 公佈之現有的加拿大註冊會計師（CPA）WebTrust 計劃。

“通用版”就一張數碼證書（伺服器）而言，指在證書所載之伺服器名稱的完整格式網域名稱的最左邊部份指定為通
配符（即星號“*”），使證書可用於登記人機構所擁有的同一域名或子域名的所有伺服器名稱。

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機關 “HKCA d-Cert DV SSL CA 2 - 25” 、 “HKCA d-Cert OV SSL CA 2 - 25” 及 “HKCA d-Cert EV SSL CA 2 - 25” 根據本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機關或根據其他核證作業準則發出的數碼證書格式，請根據該數碼證書上的發出日期或其「證書政策」內所載之物件識別碼（OID），查閱相關版本的核證作業準則。

1) 根源證書 “HKCA Root CA 2” 之下的數碼證書（伺服器）格式

以下為適用於由中繼證書" HKCA d-Cert DV SSL CA 2 - 25” 簽發的域名認證數碼證書（伺服器）:-

欄位名稱		**欄位內容**		
標準欄 (Standard fields)		**域名認證數碼證書（伺服器）**	**域名認證數碼證書（伺服器）“通用版”**	**域名認證數碼證書（伺服器）“多域版”**
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 DV SSL CA 2 - 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=[伺服器名稱]（附註1） 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3）				
機構信息訪問 (Authority Information Access)	**核證機關發出人(Certification Authority Issuer)**	[發出人的公開證書 URL]		
	線上證書狀態通訊規約 (OCSP)	[線上證書狀態應答 URL]（附註 10）		
機關密碼匙識別名稱 (Authority Key Identifier)		[發出人證書的主體密碼匙標識符]		
密碼匙使用方法 (Key usage)		數碼簽署，密碼匙加密		

欄位名稱		欄位內容		
標準欄 (Standard fields)		**域名認證數碼證書（伺服器）**	**域名認證數碼證書（伺服器）“通用版”**	**域名認證數碼證書（伺服器）“多域版”**
		（此欄為“關鍵”欄位）		
證書政策 (Certificate policy)（附註11）		Policy Identifier = 2.23.140.1.2.1（附註 13） Policy Identifier = [物件識別碼]（附註 4）		
主體別名 (Subject alternative name)	DNS	[主體名稱內之伺服器名稱]	[主體名稱內之伺服器名稱] + [不帶有通配符部分的伺服器名稱]（附註5）	[主體名稱內之伺服器名稱] + [0 至 49] [額外伺服器名稱]（附註6）
	rfc822	未使用		
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		
		（此欄為“關鍵”欄位）		
延伸密碼匙使用方法 (Extended key usage)		伺服器驗證		
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7）		
1.3.6.1.4.1.11129.2.4.2		證書簽署時間戳		

以下為適用於由中繼證書" HKCA d-Cert OV SSL CA 2 - 25”簽發的機構認證數碼證書（伺服器）:-

欄位名稱		欄位內容		
標準欄 (Standard fields)		**機構認證數碼證書（伺服器）**	**機構認證數碼證書（伺服器）“通用版”**	**機構認證數碼證書（伺服器）“多域版”**
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 OV SSL CA 2 - 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=[伺服器名稱]（附註1） o=[登記人機構名稱]（附註2） l=Hong Kong s=Hong kong 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		

欄位名稱		欄位內容		
標準欄 (Standard fields)		機構認證數碼證書（伺服器）	機構認證數碼證書（伺服器）“通用版”	機構認證數碼證書（伺服器）“多域版”
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3）				
機構信息訪問 (Authority Information Access)	核證機關發出人(Certification Authority Issuer)	[發出人的公開證書 URL]		
	線上證書狀態通訊規約 (OCSP)	[線上證書狀態應答 URL]（附註 10）		
機關密碼匙識別名稱 (Authority Key Identifier)		[發出人證書的主體密碼匙標識符]		
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)（附註11）		Policy Identifier = 2.23.140.1.2.2（附註 14） Policy Identifier = [物件識別碼]（附註 4）		
主體別名 (Subject alternative name)	DNS	[主體名稱內之伺服器名稱]	[主體名稱內之伺服器名稱] + [不帶有通配符部分的伺服器名稱]（附註5）	[主體名稱內之伺服器名稱] + [0 至 49] [額外伺服器名稱]（附註6）
	rfc822	未使用		
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		
		（此欄為“關鍵”欄位）		
延伸密碼匙使用方法 (Extended key usage)		伺服器驗證		
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7）		
1.3.6.1.4.1.11129.2.4.2		證書簽署時間戳		

以下為適用於由中繼證書" HKCA d-Cert EV SSL CA 2 - 25”發出的延伸認證數碼證書（伺服器）:-

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

欄位名稱		欄位內容
標準欄 (Standard fields)		
發出人 (Issuer)		cn= HKCA d-Cert EV SSL CA 2 - 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=[伺服器名稱]（附註1） o=[登記人機構名稱]（附註2） Object Identifier (2.5.4.9) =[街道地址] l=Hong Kong s=Hong kong c=HK Object Identifier (2.5.4.5) = [主體註冊編號] Object Identifier (2.5.4.15) =[業務分類，例如“私人機構”/“政府實體”/“商業實體”/“非商貿實體”]（附註11） Object Identifier (1.3.6.1.4.1.311.60.2.1.3)=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3）		
機構信息訪問 (Authority Information Access)	**核證機關發出人(Certification Authority Issuer)**	[發出人的公開證書URL]
	線上證書狀態通訊規約 (OCSP)	[線上證書狀態應答 URL]（附註9）
機關密碼匙識別名稱 (Authority Key Identifier)		[發出人證書的主體密碼匙標識符]
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 = 2.23.140.1.1（附註15） Policy Identifier = [物件識別碼]（附註4）
主體別名 (Subject alternative name)	**DNS**	[主體名稱內之伺服器名稱] + [0 至 49] [額外伺服器名稱]（附註6）
	rfc822	未使用
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
		（此欄為“關鍵”欄位）

欄位名稱		欄位內容
標準欄 (Standard fields)		
延伸密碼匙使用方法 (Extended key usage)		伺服器驗證
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9）
1.3.6.1.4.1.11129.2.4.2		證書簽署時間戳

附註：

1. 登記人機構擁有之伺服器名稱（包括伺服器的網域名稱(Domain Name)）。除英文伺服器名稱外，還支援 ISO / IEC 10646 中編碼的中文伺服器名稱字符。數碼證書（伺服器）“通用版”的伺服器名稱的完整格式網域名稱的最左邊部份必須為通配符（即星號“*”，稱為通配符部份），亦即證書可用於登記人機構所擁有的同一域名或子域名的所有伺服器名稱，例如：*.hkca.hk, *.subdomain.hkca.hk 。
2. 數碼證書（伺服器）以英文發行，機構名稱為英文或中文。申請數碼證書並在申請表格中提供其公司中文名稱的機構，他們可決定是否在數碼證書上顯示中文公司名稱。如機構未有提供此區分，則該公司的英文名稱將顯示在其數碼證書內。對於只有中文公司名稱的公司申請數碼證書，或只提供中文公司名稱的公司，其中文公司名稱會顯示在數碼證書內（見本核證作業準則第 3.1.1.3 條）。此外，機構分行/部門名稱將以公司名稱的相同語言顯示。除非另有說明，否則所有標準延伸均設為“非關鍵”。
3. 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。
4. 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，請參閱第 1.2 條。
5. 數碼證書（伺服器）“通用版”的主體別名包含二個伺服器名稱，一個為顯示在主體名稱內之伺服器名稱，其完整格式網域名稱的最左邊部份帶有通配符（即星號“*”，稱為通配符部份），另一個為不帶通配符部份的伺服器名稱（例如：*.hkca.hk and hkca.hk ）。除英文伺服器名稱外，還支援帶有 ISO / IEC 10646 編碼字符的中文伺服器名稱。
6. 數碼證書（伺服器）“多域版”之主體別名可包含多至 50 個伺服器名稱，第一個是顯示在主體名稱內的伺服器名稱，及可包含 0 至 49 個額外伺服器名稱。任何帶有通配符（即星號“*”）之伺服器名稱將不會被接受。除英文伺服器名稱外，還支援 ISO / IEC 10646 中編碼的中文伺服器名稱字符。
7. 對於由中繼證書" HKCA d-Cert DV SSL CA 2 - 25"所發出的證書，證書撤銷清單分發點 URL 為 http://crl.hkca.hk/crl/HKCAdCertDVSSLCA2-25CRL.crl，此乃中繼證書" HKCA d-Cert DV SSL CA 2 - 25"所發出的「整體證書撤銷清單」。
8. 對於由中繼證書"HKCA d-Cert OV SSL CA 2 - 25"所發出的證書，證書撤銷清單分發點 URL 為 http://crl.hkca.hk/crl/HKCAdCertOVSSLCA2-25CRL.crl，此乃中繼證書"HKCA d-Cert OV SSL CA 2 - 25"所發出的「整體證書撤銷清單」。
9. 對於由中繼證書"HKCA d-Cert EV SSL CA 2 - 25"所發出的證書，證書撤銷清單分發點 URL 為 http://crl.hkca.hk/crl/HKCAdCertEVSSLCA2-25CRL.crl，此乃中繼證書"HKCA d-Cert EV SSL CA 2 - 25"所發出的「整體證書撤銷清單」。
10. 線上證書狀態通訊規約應答伺服器的 URL 為 http://ocsp.hkca.hk
11. 本欄包含以下字串其中之一：“私人機構”、“政府實體”、“商業實體”或“非商貿實體”，具體視乎登記人機構是否符合延伸認證 SSL 證書準則的相關條款。
12. 由中繼證書簽發的證書符合本準則和核證機關/瀏覽器論壇基線要求。
13. 此欄位中添加了核證機關/瀏覽器論壇物件識別碼，用於標識根據核證機關/瀏覽器論壇基線要求發出的域名認證證書。
14. 此欄位中添加了核證機關/瀏覽器論壇物件識別碼，用於標識根據核證機關/瀏覽器論壇基線要求發出的證書組織標
識聲明。
15. 此欄位中添加了核證機關/瀏覽器論壇對延伸認證 SSL 證書準則的物件識別碼，用於標識證書。

附錄 C

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)

本附錄 C 詳述有關由中繼證書“HKCA d-Cert DV SSL CA 2 - 25”，“HKCA d-Cert OV SSL CA 2 - 25”及“HKCA d-Cert EV SSL 2 - 25”所發出的證書撤銷清單，以及由根源證書" HKCA Root CA 2"所發出的授權撤銷清單的更新及公佈安排和其格式。

香港數碼證書頒發中心每天三次更新及公佈的證書撤銷清單（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撤銷的數碼證書的資訊：

a) **「整體證書撤銷清單」(Full CRL)** 包含分別由中繼證書 HKCA d-Cert DV SSL CA 2 - 25”，“HKCA d-Cert OV SSL CA 2 - 25”及“HKCA d-Cert EV SSL 2 - 25”所發出的所有已撤銷證書的資料。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 DV SSL CA 2 - 25"所發出的證書：
http://crl.hkca.hk/crl/HKCAdCertDVSSLCA2-25CRL.crl 或
dap://ldap.hkca.hk (port 389, cn=HKCA d-Cert DV SSL CA 2 - 25 CRL, o=Hong Kong Internet Registration Corporation Limited, c=HK)

ii. 由中繼證書" HKCA d-Cert OV SSL CA 2 - 25"所發出的證書：
http://crl.hkca.hk/crl/HKCAdCertOVSSLCA2-25CRL.crl 或
ldap://ldap.hkca.hk (port 389, cn=HKCA d-Cert OV SSL CA 2 - 25 CRL, o=Hong Kong Internet Registration Corporation Limited, c=HK)

iii 由中繼證書" HKCA d-Cert EV SSL CA 2 - 25"所發出的證書：
http://crl.hkca.hk/crl/HKCAdCertEVSSLCA2-25CRL.crl 或
ldap://ldap.hkca.hk (port 389, cn=HKCA d-Cert EV SSL CA 2 - 25 CRL, o=Hong Kong Internet Registration Corporation Limited, c=HK)

上述的證書撤銷清單包含已撤銷證書的資料，公眾可於證書的「證書撤銷清單分發點」(CRL distribution points) 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 https://www.hkca.hk/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佈授權撤銷清單，而清單內載有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佈。最新發出的授權撤銷清單可於下述位置下載：

i. 由根源證書" HKCA Root CA 2"所發出的證書：
http://crl.hkca.hk/crl/HKCARootCA2ARL.crl 或
ldap://ldap.hkca.hk (port 389, cn=HKCA Root CA 2 ARL, o=Hong Kong Internet Registration Corporation Limited, c=HK)

(I) 由中繼證書" HKCA d-Cert DV SSL CA 2 - 25"根據本準則發出的證書撤銷清單格式:-

標準欄位 (Standard fields)	子欄位 (Sub-fields)	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 DV SSL CA 2 - 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，證書撤銷清單是每日更新及發出
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 3）			
機關密碼匙識別名稱 (Authority Key Identifier)		[簽發此證書撤銷清單之中繼證書的主體密碼匙標識符]	
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。

(II) 由中繼證書" HKCA d-Cert OV SSL CA 2 - 25"根據本準則發出的證書撤銷清單格式:-

標準欄位 (Standard fields)	子欄位 (Sub-fields)	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 OV SSL CA 2 - 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，證書撤銷清單是每日更新及發出

標準欄位 (Standard fields)	子欄位 (Sub-fields)	證書撤銷清單欄位內容	備註
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 3）			
機關密碼匙識別名稱 (Authority Key Identifier)		[簽發此證書撤銷清單之中繼證書的主體密碼匙標識符]	
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。

(III) 由中繼證書" HKCA d-Cert EV SSL CA 2 - 25”根據本準則發出的證書撤銷清單格式:-

標準欄位 (Standard fields)	子欄位 (Sub-fields)	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 EV SSL CA 2 - 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**每日**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 3）			
機關密碼匙識別名稱 (Authority Key Identifier)		[簽發此證書撤銷清單之中繼證書的主體密碼匙標識符]	
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。

(IV) 由根源證書" HKCA Root CA 2"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

標準欄位 (Standard fields)	子欄位 (Sub-fields)	授權撤銷清單欄位內容	備註
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 2 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
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 2）
標準延伸欄位 (Standard extension) （附註 3）			
機關密碼匙識別名稱 (Authority Key Identifier)		[簽發此授權撤銷清單之根源證書的主體密碼匙標識符]	
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。

附注

1. 有關數碼證書（伺服器）的證書撤銷清單，其證書撤銷清單資料延伸欄位可包含以下撤銷理由識別碼：

   1 = 密碼匙資料外洩，3 = 聯繫變更，4 = 證書被取代，
   5 = 終止營運，9 = 特權被撤銷

   否則，證書撤銷清單資料延伸欄位不會包含撤銷理由識別碼。

2. 有關根源證書及中繼證書的授權撤銷清單，其證書撤銷清單資料延伸欄位必須包含以下其中一個撤銷理由識別碼：

   0 = 沒有註明，1 = 密碼匙資料外洩，2 = 核證機關資料外洩，3 = 聯繫變更，
   4 = 證書被取代，5 = 終止營運

3. 除非另有說明，否則所有欄位均將設定為“非關鍵”。

附錄 D - 香港數碼證書頒發中心線上證書狀態應答(OCSP Response)格式

本附錄 D 詳述有關香港數碼證書頒發中心線上證書狀態應答(OCSP Response)格式

通過發佈一個包含以下主體名稱的線上證書狀態通訊規約簽署人證書，香港數碼證書頒發中心已授權一個線上證書狀態通訊規約應答伺服器為根源證書 CA 及中繼證書進行線上證書狀態通訊規約的簽署。

根源證書：

證書主體名稱 (CN)	**線上證書狀態通訊規約簽署人證書主體名稱 (CN)**
"HKCA Root CA 2"	"HKCA Root CA 2 OCSP Responder"

中繼證書：

證書主體名稱 (CN)	**線上證書狀態通訊規約簽署人證書主體名稱 (CN)**
"HKCA d-Cert DV SSL CA 2 - 25"	"HKCA d-Cert DV SSL CA 2 - 25 OCSP Responder"
"HKCA d-Cert OV SSL CA 2 - 25"	"HKCA d-Cert OV SSL CA 2 - 25 OCSP Responder"
"HKCA d-Cert EV SSL CA 2 - 25"	"HKCA d-Cert EV SSL CA 2 - 25 OCSP Responder"

除此以外，線上證書狀態通訊規約應答伺服器獲分配了一個唯一的物件識別碼 OID **"1.3.6.1.4.1.64092.1.6"**，指定於線上證書狀態通訊規約簽署人證書的"證書政策" 欄位。在附錄 D 的最後章節，還將提供線上證書狀態應答的格式。

香港數碼證書頒發中心線上證書狀態通訊規約應答伺服器只支持基本的線上證書狀態應答類型。一個明確的線上證書狀態應答數據由以下組成：

標準欄位 (Standard Fields)	**子欄位(Sub-fields)**	**子欄位(Sub-fields)**	**欄位內容**	**備註**
應答數據 (Response data)	版本(Version)		v1 (0x0)	
	應答伺服器識別 Responder ID	by key 憑密碼匙	[應答伺服器的公匙 SHA-1 雜湊值]	
	Produced At 產生於		[Generalized 時間]	此應答簽署的時間 (GMT+0)
	Sequence of Single Response 單一應答的序列			
	Single Response 單一應答	Certificate ID 證書識別	[要求的證書識別名稱]	要求的證書識別名稱包含： • 雜湊函數識別 • 發出人主體名稱的雜湊值 • 發出人公匙的雜湊值 • 證書序號
		證書狀態 (Certificate status)	[證書的狀態]	有效、撤銷（附有日期、時間(GMT+0)和撤銷原因代碼（附註 1，2））或未知
		本次更新 This update	[Generalized 時間]	證書正確狀態的最近日期和時間 (GMT+0)
		下次更新 Next update	[Generalized 時間]	更新證書狀態的日期和時間 (GMT+0)

標準欄位 (Standard Fields)	子欄位(Sub-fields)	子欄位(Sub-fields)	欄位內容	備註
簽署算式識別 (Signature algorithm ID)			sha256RSA	用於簽署此應答的算法
簽署(Signature)			[簽署數據]	應答的簽名
證書(Certificate)			[應答伺服器簽署人證書的數據]	應答伺服器的簽署人證書

附註：

1. 有關數碼證書(伺服器)的線上證書狀態應答，其證書狀態欄位可包含以下撤銷理由識別碼：

   0 = 沒有註明，1 = 密碼匙資料外洩，3 = 聯繫變更，4 = 證書被取代，
   5 = 終止營運，9 = 特權被撤銷

2. 有關根源證書及中繼證書的線上證書狀態應答，其證書狀態欄位必須包含以下其中一個撤銷理由識別碼：

   0 = 沒有註明，1 = 密碼匙資料外洩，2 = 核證機關資料外洩，3 = 聯繫變更，
   4 = 證書被取代，5 = 終止營運

附錄 E - 香港數碼證書頒發中心數碼證書 – 認證類型摘要

要點	域名認證數碼證書(伺服器)	機構認證數碼證書(伺服器)	延伸認證數碼證書(伺服器)
登記人	獲香港特別行政區政府簽發有效商業登記證之機構、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	即登記人		
依據限額	HK$ 0	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	由登記人自行產生		
核對身分	核對網域名稱(Domain Name)及其獲授權代表的身分	核對網域名稱(Domain Name)、機構及其獲授權代表的身分	核對機構的合法存在、實體存在和營運存在、通信方法，核實域名身份及核實其獲授權代表
證書用途	數碼簽署及數據加密		
證書內包含登記人的資料	• 登記人機構之伺服器名稱及在主體別名內列出之額外伺服器名稱	• 登記人機構名稱 • 登記人機構之伺服器名稱及在主體別名內列出之額外伺服器名稱	• 登記人機構名稱、街道地址及業務類別 • 登記人機構之伺服器名稱及在主體別名內列出之額外伺服器名稱
登記及行政費用	見本核證作業準則第 9.1 條		
證書有效期	199 天		
	（見本核證作業準則第 4.6.1 及 6.3.2 條）		

附錄 F - 香港數碼證書頒發中心數碼證書核證登記機關名單（若有的話）

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 G - 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 H - 核證機關根源證書的有效期

參考項目	香港數碼證書頒發中心核證機關根源證書名稱	有效期	備註
1	HKCA Root CA 2	2025 年 10 月 20 日 至 2050 年 10 月 14 日	
主體專有名稱 （Subject DN） C=HK, ST=Hong Kong, L=Hong Kong, O=Hong Kong Internet Registration Corporation Limited, CN=HKCA Root CA 2 SHA-1 Thumbprint E3:3E:C1:E1:26:FB:4F:E2:B6:1D:B7:8E:8A:EE:AD:6D:8E:BF:8E:84 SHA-256 Thumbprint 98:90:08:22:A3:D6:A9:7B:D8:31:0D:05:70:F1:E6:A5:51:B6:B8:35:6F:FE:3D:4E:82:58:23:8E:22:86:C0:6A			
2	HKCA d-Cert DV SSL CA 2 - 25	2025 年 12 月 4 日 至 2040 年 11 月 30 日	此中繼證書由 XXXX 年 X 月 X 日起開始發出域名認證數碼證書（伺服器）。
主體專有名稱 （Subject DN） C=HK, ST=Hong Kong, L=Hong Kong, O=Hong Kong Internet Registration Corporation Limited, CN=HKCA d-Cert DV SSL CA 2 - 25 SHA-1 Thumbprint 69:CA:D8:BB:F7:BB:96:CA:6E:E3:6D:68:A4:6B:B9:FF:02:E7:2B:C6 SHA-256 Thumbprint 6C:B0:1D:5B:11:20:1C:5E:5D:BD:E2:EB:0A:45:D4:00:AE:F3:FF:5E:EF:63:90:76:B9:E8:38:2D:F3:B7:92:69			
3	HKCA d-Cert OV SSL CA 2 - 25	2025 年 12 月 4 日 至 2040 年 11 月 30 日	此中繼證書由 XXXX 年 X 月 X 日起開始發出機構認證數碼證書（伺服器）。

參考項目	香港數碼證書頒發中心核證機關根源證書名稱	有效期	備註
主體專有名稱 （Subject DN） C=HK, ST=Hong Kong, L=Hong Kong, O=Hong Kong Internet Registration Corporation Limited, CN=HKCA d-Cert OV SSL CA 2 - 25 SHA-1 Thumbprint 05:40:36:DC:88:2C:12:C8:ED:1C:49:7E:B9:CB:35:93:58:8D:A0:6A SHA-256 Thumbprint C5:F4:88:39:B2:14:94:A1:16:9D:36:FB:0C:52:D1:98:FD:3F:62:DF:1D:2E:21:79:E0:94:1E:4F:B6:08:41:52			
4	HKCA d-Cert EV SSL CA 2 - 25	2025 年 12 月 4 日 至 2040 年 11 月 30 日	此中繼證書由 XXXX 年 X 月 X 日起開始發出延伸認證數碼證書（伺服器）。
主體專有名稱 （Subject DN） C=HK, ST=Hong Kong, L=Hong Kong, O= Hong Kong Internet Registration Corporation Limited, CN=HKCA d-Cert EV SSL CA 2 - 25 SHA-1 Thumbprint 4F:CE:70:57:A4:DC:45:07:A6:3A:01:26:E8:73:17:90:51:B8:23:5D SHA-256 Thumbprint 97:7B:CE:D8:9D:7B:83:75:1D:65:0E:C3:B6:FD:94:72:B7:13:B2:3B:8E:C1:FC:EC:0F:96:6D:53:67:7E:44:5E			

此為本核證作業守則之最終頁