以香港郵政署長
根據電子交易條例作為認可核證機關

之

香港郵政
電子證書（個人）
電子證書（機構）
電子證書（保密）

核證作業準則

日期：二零二六年十一月二十五日
物件識別碼：1.3.6.1.4.1.16030.1.1.58

目錄

前言 9
1． 引言 11
1.1 概述 11
1.2 文件名稱及識別資料 11
1.3 公匙基建參與者 12
1.3.1 核證機關 12
1.3.2 核證登記機關 12
1.3.3 登記人 12
1.3.4 倚據人士 14
1.3.5 其他參與者 14
1.4 證書用途 14
1.4.1 證書的適用用途 14
1.4.2 證書的禁止用途 14
1.5 策略管理 15
1.5.1 管理本文件的機構 15
1.5.2 聯絡人 15
1.5.3 決定核證作業準則是否符合策略的人 15
1.5.4 核證作業準則的審批程序 15
1.6 定義和縮寫 15
2． 公開資料及儲存庫責任 16
2.1 儲存庫 16
2.2 認證資料公布 16
2.2.1 互認證書的互認信任列表 16
2.3 公布時間或頻率 16
2.4 儲存庫進入控制 16
3． 鑑別及認證 17
3.1 命名 17
3.1.1 名稱類型 17
3.1.2 名稱需有意義 18
3.1.3 登記人的匿名或假名 18
3.1.4 詮釋名稱規則 18
3.1.5 名稱獨特性 18
3.1.6 商標的認可、驗證及角色 18
3.2 初始身分驗證 18
3.2.1 證明擁有私人密碼匙之方法 19
3.2.2 組織機構身分認證 19
3.2.3 個人身分認證 20
3.2.4 沒有驗證的登記人資訊 20
3.2.5 權限及郵箱控制驗證 20
3.2.6 互操作準則 20
3.3 密碼匙更新請求的標識與鑒別 20
3.3.1 常規密碼匙更新時的身分識別及身分認證 20
3.3.2 證書撤銷後密碼匙更新時的身分識別及身分認證 20
3.4 撤銷請求的身分識別及身分認證 21

4 · 證書生命週期操作要求 22
4.1 證書申請 22
4.1.1 誰能遞交證書申請 22
4.1.2 登記過程與責任 22
4.2 處理證書申請 22
4.2.1 履行鑒別及認證職能 22
4.2.2 證書申請批准和拒絕 24
4.2.3 證書申請的處理期限 24
4.3. 證書簽發 25
4.3.1 證書簽發期間核證機關的行為 25
4.3.2 電子認證服務機構和註冊機構對登記人的通告 26
4.4 證書接受 26
4.4.1 構成接受證書的行為 26
4.4.2 核證機關對證書的發布 26
4.4.3 核證機關對其他實體的通告 26
4.5 配對密碼匙和證書的使用 26
4.5.1 登記人私人密碼匙和證書的使用 26
4.5.2 倚據人士公開密碼匙和證書的使用 26
4.6 證書續期 27
4.6.1 證書續期的情形 27
4.6.2 誰能要求證書續期 27
4.6.3 證書續期請求的處理 27
4.6.4 發出新證書時對登記人的通告 28
4.6.5 構成接受續期證書的行為 28
4.6.6 核證機關對續期證書的發布 28
4.6.7 核證機關對其他實體的通告 28
4.7 證書密碼匙更新 28
4.7.1 證書密碼匙更新的情形 28
4.7.2 誰能要求證書公開密碼匙更新 28
4.7.3 證書密碼匙更新請求的處理 28
4.7.4 發出新證書時對登記人的通告 29
4.7.5 構成接受密碼匙更新證書的行為 29
4.7.6 核證機關對密碼匙更新證書的發布 29
4.7.7 核證機關對其他實體的通告 29
4.8 證書變更 29
4.8.1 證書變更的情形 29
4.8.2 請求證書變更的實體 29
4.8.3 證書變更請求的處理 29
4.8.4 發出新證書時對登記人的通告 29
4.8.5 構成接受變更證書的行為 29
4.8.6 核證機關對變更證書的發佈 29
4.8.7 核證機關對其他實體的通告 29
4.9 證書撤銷和暫時吊銷 29
4.9.1 證書撤銷的情形 29
4.9.2 誰能要求證書撤銷 31

4.9.3 撤銷請求的程序 31
4.9.4 撤銷請求寬限期 32
4.9.5 核證機關處理撤銷請求的時限 32
4.9.6 供倚據人士檢查證書撤銷的規定 32
4.9.7 證書撤銷清單發布頻率 33
4.9.8 發佈證書撤銷清單的最大滯後時間 33
4.9.9 線上撤銷／狀態查詢的可用性 33
4.9.10 線上撤銷查詢規定 33
4.9.11 撤銷公告的其他發布形式 33
4.9.12 密碼匙資料外洩的特殊規定 33
4.9.13 證書暫時吊銷的情形 33
4.9.14 誰能要求暫時吊銷證書 33
4.9.15 要求暫時吊銷的程序 34
4.9.16 暫時吊銷的期限限制 34
4.10 證書狀態服務 34
4.10.1 操作特徵 34
4.10.2 服務可用性 34
4.10.3 運作特點 34
4.11 登記使用期結束 34
4.12 密碼匙托管與復原 34
4.12.1 密碼匙託管與復原的策略及實施 34
4.12.2 工作階段密碼匙封裝及復原政策與實施 35
5． 設施、管理和運作控制 36
5.1 實體控制 36
5.1.1 選址及建造 36
5.1.2 實體訪問 36
5.1.3 電力及空調 36
5.1.4 水患 36
5.1.5 火災防護 36
5.1.6 媒體存儲 36
5.1.7 廢物處理 36
5.1.8 場外備存 36
5.2 程序控制 37
5.2.1 受信職責 37
5.2.2 每項任務需要的人數 37
5.2.3 每個角色的鑑別及認證 37
5.2.4 需要職責分割的角色 37
5.3 人員控制 37
5.3.1 資格、經驗和無過失要求 37
5.3.2 背景調查程序 37
5.3.3 培訓要求 37
5.3.4 再培訓週期和要求 37
5.3.5 工作崗位輪換週期和順序 38
5.3.6 未授權行為的處罰 38
5.3.7 獨立承辦商的要求 38

5.3.8 向人員提供之文件 38
5.4 審計日誌程序 38
5.4.1 記錄事件類型 38
5.4.2 處理紀錄之次數 39
5.4.3 審核紀錄之存留期間 39
5.4.4 審核紀錄之保護 39
5.4.5 審核紀錄備存程序 39
5.4.6 審核收集系統（內部對外部） 39
5.4.7 事件主體的通告 39
5.4.8 脆弱性評估 39
5.5 紀錄存檔 39
5.5.1 存檔紀錄類型 39
5.5.2 存檔保存期限 40
5.5.3 存檔保護 40
5.5.4 存檔備份程序 40
5.5.5 電子郵戳的要求 40
5.5.6 存檔收集系統（內部對外部） 40
5.5.7 獲取及驗證存檔資料的程序 40
5.6 密碼匙變更 40
5.7 資料外洩與災難復原 40
5.7.1 事故和資料外洩處理程序 40
5.7.2 計算機資源、軟件和／或數據的損壞 41
5.7.3 私人密碼匙資料外洩之程序 41
5.7.4 災難後的持續營運能力 41
5.8 核證機關或核證登記機關終止服務 42
6． 技術保安控制 43
6.1 密碼匙之產生及安裝 43
6.1.1 產生配對密碼匙 43
6.1.2 私人密碼匙交付予登記人 43
6.1.3 公開密碼匙交付予證書發出人 43
6.1.4 核證機關公開密碼匙交付予倚據人士 43
6.1.5 密碼匙大小 43
6.1.6 公開密碼匙參數的生成和品質檢查 43
6.1.7 密碼匙用途（按照 X.509 v3 密碼匙使用方法欄位） 43
6.2 私人密碼匙保護和加密模組控制 44
6.2.1 加密模組的標準和控制 44
6.2.2 私人密碼匙（m 選 n）多人式控制 44
6.2.3 私人密碼匙托管 44
6.2.4 私人密碼匙備存 44
6.2.5 私人密碼匙存檔 44
6.2.6 私人密碼匙於密碼模組之間傳遞 44
6.2.7 私人密碼匙在加密模組的存儲 44
6.2.8 啟動私人密碼匙的方法 44
6.2.9 停用私人密碼匙的方法 44
6.2.10 銷毀私人密碼匙的方法 44

6.2.11 加密模組的評估 44
6.3 配對密碼匙管理其他範疇 44
6.3.1 公開密碼匙存檔 45
6.3.2 證書操作期和配對密碼匙使用期限 45
6.4 啟動數據 45
6.4.1 啟動數據的產生和安裝 45
6.4.2 啟動數據的保護 45
6.4.3 激活數據的其他範疇 45
6.5 電腦保安控制 45
6.5.1 特定電腦保安技術要求 45
6.5.2 電腦安全評估 45
6.6 生命週期技術控制 46
6.6.1 系統開發控制 46
6.6.2 保安管理控制 46
6.6.3 生命週期的保安控制 46
6.7 網絡保安控制 46
6.8 電子郵戳 46
7． 證書、證書撤銷清單及線上證書狀態應答結構 47
7.1 證書結構 47
7.1.1 版本編號 47
7.1.2 證書延伸欄位 47
7.1.3 算式物件識別碼 47
7.1.4 名稱格式 47
7.1.5 名稱限制 47
7.1.6 證書策略物件識別碼 47
7.1.7 策略限制延伸欄位使用的政策 47
7.1.8 策略限定資格的語法和語義的政策 47
7.1.9 關鍵證書策略延伸欄位的語義處理 47
7.2 證書撤銷清單結構 47
7.2.1 版本編號 50
7.2.2 證書撤銷清單及證書撤銷清單資料延伸欄位 50
7.3 線上證書狀態應答結構 51
7.3.1 版本編號 51
7.3.2 線上證書狀態應答延伸欄位 51
8． 遵守規定審核和其他評估 52
8.1 評估的頻率及情形 52
8.2 評估者的資格 52
8.3 評估者與被評估實體之間的關係 52
8.4 評估內容 52
8.5 對問題與不足採取的措施 52
8.6 評估結果的傳達與發布 52
8.7 自我審核 52
9． 法律責任和其他業務條款 53
9.1 費用 53
9.1.1 證書簽發和續期費用 53

9.1.2 證書查詢費用 54
9.1.3 證書撤銷或狀態資訊的查詢費用 54
9.1.4 其他服務費用 54
9.1.5 退款政策 55
9.2 財務責任 55
9.2.1 保險範圍 55
9.2.2 其他資產 55
9.2.3 對最終實體的保險或擔保 55
9.3 業務資料機密 55
9.3.1 機密資料範圍 55
9.3.2 不屬於機密的資料 55
9.3.3 保護機密資料的責任 55
9.4 個人資料私隱 55
9.4.1 私隱方案 56
9.4.2 視作隱私的資料 56
9.4.3 不被視作私隱資料 56
9.4.4 保護私隱的責任 56
9.4.5 使用私隱資料的通告與同意 56
9.4.6 根據法律或行政程序作出的披露 56
9.4.7 其他資料披露情況 56
9.5 知識產權 56
9.6 陳述及擔保 56
9.6.1 核證機關的陳述與擔保 56
9.6.2 核證登記機關的陳述與擔保 57
9.6.3 登記人的陳述與擔保 57
9.6.4 倚據人士的陳述與擔保 58
9.6.5 其他參與者的陳述與擔保 58
9.7 免責聲明 58
9.8 有限責任 59
9.9 賠償 60
9.10 有效期限與終止 62
9.10.1 有效期限 62
9.10.2 終止 62
9.10.3 終止與保留效力 62
9.11 參與人士的個別通告與通知 62
9.12 修訂 62
9.12.1 修訂程序 62
9.12.2 通知機制和期限 63
9.12.3 必須修改物件識別碼的情形 63
9.13 爭議處理 63
9.14 管轄法律 63
9.15 符合適用法律規定 63
9.15.1 司法管轄權 63
9.16 一般條款 63
9.16.1 完整協議 63

9.16.2 轉讓 63
9.16.3 分割性 63
9.16.4 執行（不可放棄權利） 64
9.16.5 不可抗力 64
9.17 其他條款 64
9.17.1 非商品供應 64
附錄 A - 詞彙及縮寫 65
附錄 B - 香港郵政電子證書格式 69
附錄 C - 香港郵政證書撤銷清單（CRL）及香港郵政授權撤銷清單（ARL）格式 79
附錄 D - 香港郵政電子證書 – 服務摘要 83
附錄 E - 香港郵政電子證書核證登記機關名單（若有的話） 85
附錄 F - 香港郵政電子證書服務 - 翹晉電子商務有限公司之合約分判商名單（若有的話） 86
附錄 G - 核證機關根源證書的有效期 87
附錄 H - 香港郵政電子證書特定應用名單及相對應之特定應用編碼 88

©本文版權屬香港郵政署長所有。未經香港郵政署長明確許可，不得複製本文之全部或部分。

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。經公開密碼匙保護的信息只可用其配對私人密碼匙解密；而利用私人密碼匙作數碼簽署的信息亦只可用其配對公開密碼匙驗證。

設計公匙基建之目的，為支援以上述方法在香港特別行政區內進行商業活動及其他交易以及。

根據條例所載規定，香港郵政署長為認可核證機關。香港郵政署長透過香港郵政署職員履行核證機關之職能並提供服務。在本核證作業準則中，香港郵政署長稱為**香港郵政**。

自 2007 年 4 月 1 日起，香港郵政核證機關的營運已外判給私營機構承辦。香港郵政已批出合約予翹晉電子商務有限公司（“合約”），以營運和維持香港郵政核證機關的系統和服務，合約期由 2023 年 7 月 1 日至 2026 年 6 月 30 日，並延長至 2027 年 6 月 30 日（包括當日）。凡提述由香港郵政執行的所有行為，均包括由翹晉電子商務有限公司代表香港郵政執行的所有該等行為。

根據合約，在得到香港郵政的書面同意後，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）。

香港郵政依然為條例第 34 條下之認可核證機關而承辦商則為香港郵政根據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》*第 3.2 段所委任之代理人。

根據條例，香港郵政為認可核證機關，負責使用穩當系統發出、撤銷、暫時吊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證書（即電子證書（個人）、電子證書（機構）及電子證書（保密））均為條例下的認可證書，在本核證作業準則內稱為“證書”或“電子證書”。

本核證作業準則列明適用於香港郵政所發出電子證書的作業方式及標準。本核證作業準則所規管的證書僅供用戶端認證用途。

本核證作業準則獨立於規管電子證書（個人）、電子證書（機構）及電子證書（保密）有關 S/MIME 功能的香港郵政核證作業準則，亦不會取代該核證作業準則。

根據條例，香港郵政可以採取任何適當措施，以履行核證機關職能及提供核證機關服務。而根據認可核證機關作業守則，香港郵政可以指定代理人或合約分判商執行其部分或全部業務。

香港郵政可適當地指定核證登記機關為代理人，履行香港郵政作為認可核證機關於本作業準則

所列舉的特定職能。**附錄 E** 列載核證登記機關之清單（若有的話）。

除因核證登記機關疏忽、欺詐、超越其獲准權限範圍行事或其他類似情況外，香港郵政須對核證登記機關作為其代理人履行香港郵政作為認可核證機關有關發出及撤銷電子證書之職能或提供服務的行為及活動負責。

本核證作業準則列載電子證書的實務守則。

本核證作業準則符合 RFC3647 互聯網 X.509 公匙基建：證書政策及核證作業架構。

1 · 引言

1.1 概述

本核證作業準則（“準則”）由香港郵政公布，使公眾有所瞭解，本核證作業準則為一份結合證書政策（“證書政策”）及核證作業準則的文件，並規定香港郵政在發出、撤銷、暫時吊銷及公布電子證書時採用之做法及標準。

香港郵政將維護本準則，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”）相關規例和符合《粵港兩地電子簽名證書互認辦法》下的《粵港電子簽名證書互認證書政策》（“互認證書政策”）相關規定。

此外，香港郵政明確遵守最新已發布版本的《通用核證機關資料庫政策》（Common CA Database (CCADB) Policy）。倘本核證作業準則與上述政策有任何抵觸，應以上述 CCADB 政策為準。

本準則列載參與香港郵政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，並介紹香港郵政之運作、程序及保安要求。

香港郵政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。利用由香港郵政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，以供其特定應用使用。

根據條例，香港郵政為認可核證機關。**而根據本核證作業準則而發出的電子證書（個人）、電子證書（機構）及電子證書（保密），香港郵政已指明為認可證書**。其中，電子證書（個人）和電子證書（機構）分別可選包含符合互認證書策略的“互認版”功能，均是條例下的認可證書。對登記人及倚據人士而言，根據該條例香港郵政在法律上有義務使用穩當系統，發出、撤銷或暫時吊銷，以及在可供公眾使用之儲存庫公布獲接受之認可證書。

本核證作業準則符合 RFC 3647 的格式要求。雖然本核證作業準則按照 RFC 3647 的結構載有若干章節標題，但有關主題未必適用於香港郵政提供的服務。有關章節會註明“不適用”。如有需要，額外資料會載於標準結構下的分節。符合 RFC 3647 的格式要求有助與其他第三方核證機關進行對照及互操作性，並讓倚據人士預先了解香港郵政的作業方式及程序。

附錄 D 載有根據本準則發出之電子證書特點摘要。

1.2 文件名稱及識別資料

本文件為香港郵政核證機關就根據本核證準則發出的電子證書所制定的核證作業準則（“本準則”）。

香港郵政已獲 Internet Assigned Numbers Authority（IANA）分配私人企業號碼（Private Enterprise Number）16030 號。**“1.3.6.1.4.1.16030.1.1.58”** 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）。此外，香港郵政亦會在電子證書（個人）“互認版”和電子證書（機構）“互認版”的核證政策內加入數字政策辦公室指派給互認證書策略的物件識別碼（Object Identifier, OID）**“2.16.344.8.2.2008.810.2.2018.1.1”**。

1.3 公匙基建參與者

1.3.1 核證機關

根據本準則，香港郵政履行核證機關之職能並承擔其義務。香港郵政乃唯一根據本準則授權發出證書之核證機關。

香港郵政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，香港郵政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、暫時吊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，香港郵政為認可核證機關，負責使用穩當系統發出、撤銷、暫時吊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，香港郵政（或透過其委任的分判商）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） 暫時吊銷或撤銷證書並依時公布證書撤銷清單（見第 4.9 條），及
d） 通知登記人有關已暫時吊銷或撤銷的證書（見第 4.9.5 條）。

1.3.2 核證登記機關

核證登記機關遵照與香港郵政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）之條款對香港郵政負責。核證登記機關代表香港郵政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。除因疏忽、超越授權範圍行事、欺詐、刑事行為或其他類似因素外，香港郵政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郵政的功能、權力、權利和職責負責。

核證登記機關之行為僅為代表香港郵政履行香港郵政於此等事項之義務及責任。核證登記機關有權代表香港郵政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）。

附錄 E 載有香港郵政電子證書核證登記機關清單（若有的話）。

1.3.3 登記人

根據本準則，登記人指**附錄 A** 所述的“登記人”或“登記人機構”。

1.3.3.1 登記人類別

根據本準則香港郵政僅發出證書予其申請已獲香港郵政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。三類電子證書會根據本準則而發出。

1.3.3.1.1 電子證書（個人）

電子證書（個人）根據本準則及登記人協議發給持有香港身分證的人士（即“登記人”）。

此類證書可作為登入伺服器或網上平台、遞交申請或文件存檔，以及透過政府電子採購系統遞交投標書的身分證明。配合適當的第三方軟件，此類證書亦可用作對電子文件進行數碼簽署。

此外，電子證書（個人）“互認版”所產生的數碼簽署，設計上可獲 Adobe 文件簽署軟件的信任，並適用於《粵港電子簽名證書互認安排》下的適用範圍。“互認版”證書在《中華人民共和國電子簽名法》適用範圍內，於廣東省內享有與廣東省認可核證機關所發出證書同等的法律地位。詳情請參閱 https://www.digitalpolicy.gov.hk/en/our_work/digital_infrastructure/mainland/cepa/mr_ecert/。

電子證書（個人）亦可發給持有香港身分證而年齡未滿 18 歲的人士（另見**第 3.1.1.2 條**）。電子證書（個人）“互認版”不得發給年齡未滿 18 歲的人士。

1.3.3.1.2 電子證書（機構）

電子證書（機構）發給：

(i) 香港特別行政區政府各政策局及部門；
(ii) 持有由香港特別行政區政府發出的有效商業登記證之機構，或持有香港特別行政區政府稅務局向《稅務條例》（第 112 章）所述申報財務機構／申報實體／第 4AA 部實體發出的有效證明書之機構；及
(iii) 獲香港法例認可存在之本港法定團體（各稱為“登記人機構”）；

並識別已獲該登記人機構授權使用該電子證書（機構）私人密碼匙的成員或僱員（即“授權用戶”）。

此類證書可作為登入伺服器或網上平台、遞交申請或文件存檔，以及透過政府電子採購系統遞交投標書的身分證明。配合適當的第三方軟件，此類證書亦可用作對電子文件進行數碼簽署。此外，電子證書（機構）“互認版”所產生的數碼簽署，設計上可獲 Adobe 文件簽署軟件信任，並適用於《粵港電子簽名證書互認安排》下的適用範圍。電子證書（機構）“互認版”不得發給年齡未滿 18 歲的人士。

登記人機構向香港郵政承諾，不會授權授權用戶將電子證書（機構）用於**上述用途**以外的任何用途。

就電子證書（機構）而言，申請人可申請具自動交換資料（AEOI）功能的電子證書（機構）。該證書為載有特定代碼“IRD_AEOI”的電子證書（機構）。AEOI 平台為稅務局指定供財務機構遞交通知及財務帳戶資料申報表的系統。具 AEOI 功能的電子證書（機構）供財務機構／申報實體／第 4AA 部實體使用，而只有具 AEOI 功能的電子證書（機構）方可登入稅務局 AEOI 平台下的 AEOI 帳戶，該用途即**附錄 H** 所述之指定應用。

持有香港特別行政區政府稅務局向《稅務條例》（第 112 章）所述申報財務機構／申報實體／第 4AA 部實體發出的有效證明書之登記人機構，向香港郵政承諾，不會授權授權用戶將電子證書（機構）用於上述用途以外的任何用途，或於**附錄 H** 所述的指定應用內產生數碼簽署。

1.3.3.1.3 電子證書（保密）

電子證書（保密）發給：

(i) 香港特別行政區政府各政策局及部門；
(ii) 持有由香港特別行政區政府發出的有效商業登記證之機構；及
(iii) 獲香港法例認可存在之本港法定團體（各稱為“登記人機構”）。

此類證書擬供已獲登記人機構授權使用電子證書（保密）私人密碼匙之機構單位（“授權單位”）使用。

此類證書可用於進行伺服器與伺服器之間的安全通訊。此類證書並不具備對文件執行數碼簽署所需的技術規格及法律合規框架。

登記人機構向香港郵政承諾，不會授權授權單位將電子證書（保密）用於**上述用途**以外的任何用途。

1.3.4 倚據人士

倚據人士乃倚據香港郵政發出之任何類別或種類證書，包括但不限於用作核實數碼簽署之電子證書。

1.3.5 其他參與者

只要分判商同意與香港郵政簽訂合約承擔有關職務，香港郵政可把履行本準則及登記人協議之部分或全部工作之義務，批予分判商執行。若發生此類分判情況，除因疏忽、超出授權範圍行事、欺詐、犯罪行為或其他類似因素導致的情況外，香港郵政仍須就本準則及登記人協議的履行承擔責任，猶如未進行該等分判一樣。

如上所述，翹晉電子商務有限公司及其分判商（統稱為“承辦商”）確實為香港郵政委任的分判商之一。

承辦商祇會依據香港郵政及承辦商之合約條款，包括承辦商作為香港郵政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、推廣及維持香港郵政核證機關之系統及服務，而對香港郵政負責。除因疏忽、超越授權範圍行事、欺詐、刑事行為或其他類似因素外，香港郵政會依然對承辦商在其執行或將會執行香港郵政之功能權力，權利及職能之行為負責。

附錄 F 載有香港郵政電子證書服務 - 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 證書的適用用途

根據本準則香港郵政僅發出證書予其申請已獲香港郵政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。

根據本準則發出的電子證書僅供第 1.3.3.1 條所述用途使用。

1.4.2 證書的禁止用途

根據本準則發出的電子證書不得用於安全電子郵件通訊。

1.5 策略管理

1.5.1 管理本文件的機構
本準則由香港郵政公布，使公眾有所瞭解，並規定香港郵政在發出、撤銷、暫時吊銷及公布證書時採用之做法及標準。

1.5.2 聯絡人
登記人可經由以下途徑作出查詢、建議或投訴：

郵寄地址：東九龍郵政信箱 68777 號香港郵政核證機關
電話 ：2921 6633
傳真 ：2775 9130
電郵地址 ：enquiry@eCert.gov.hk

香港郵政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，香港郵政會向投訴人作出簡覆。在可行範圍內，香港郵政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 決定核證作業準則是否符合策略的人
香港郵政將維護本準則，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 核證作業準則的審批程序
本準則之更改一律須經香港郵政核准及公布。香港郵政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

本準則所使用的定義及縮寫載於**附錄 A**。

2． 公開資料及儲存庫責任

2.1 儲存庫

根據條例之規定，香港郵政維持一可供公眾查閱的儲存庫，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、證書撤銷清單（CRLs），香港郵政公開密碼匙、本準則文本一份以及與本準則電子證書有關之其他資料，包括電子證書申請表及其中包含的《登記人條款及條件》。香港郵政會盡快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。

儲存庫內的資料（包括任何個人資料）乃根據條例發布，以便利進行合法電子通訊。

2.2 認證資料公布

香港郵政儲存庫可透過下述 URL 接達：

http://www.eCert.gov.hk
ldap://ldap1.eCert.gov.hk

或

http://www.hongkongpost.gov.hk
ldap://ldap1.hongkongpost.gov.hk

2.2.1 互認證書的互認信任列表

香港郵政已指定電子證書（個人）“互認版”及電子證書（機構）“互認版”參與《粵港兩地電子簽名證書互認辦法》下的證書互認計劃。有關具互認資格的特定證書類別及這些證書類別的身份審核方式，請參閱廣東省經濟和信息化委員會發佈的官方信任列表，以確定證書類別是否具互認資格及其有效期。數字政策辦公室亦會在其信任列表備存有關資料的副本，以供參考。

2.3 公布時間或頻率

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等其他相關情況時，儲存庫會盡快作出更新。

除不時作出的其他修訂外，香港郵政最少每 365 日檢討及更新本準則，並作出適當修訂，以確保香港郵政的運作保持準確、透明及符合本文件 *“引言”* 部分所列的外部要求。此準則的新版本或修改版通常在其批准後七（7）天內發布。

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。

經授權之香港郵政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，香港郵政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

本節說明根據本準則發出的電子證書申請人及登記人所適用的身分識別及身分認證要求。

3.1 命名

根據本準則發出的電子證書會按照**附錄 B** 所訂明的命名規則及證書結構，利用主體名稱識別登記人。

3.1.1 名稱類型

3.1.1.1 電子證書（個人）

透過證書上的主體名稱（於附錄 B 內指明），可識別電子證書（個人）登記人之身分。該名稱由登記人香港身份證上顯示的姓名組成。

登記人的香港身份證號碼將以雜湊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簽發電子證書（個人）

透過證書上的主體名稱（於**附錄 B** 內指明）可識別不屬於電子證書（個人）“互認版”登記人之身分，該名稱由以下資料組成：

a）第 3.1.1.1 條所指明的主體名稱；及
b）使用“電子證書（個人／未成年人）”此表述（見附錄 B），以顯示登記人在證書發出時未滿 18 歲。

3.1.1.3 電子證書（機構）

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

a) 授權用戶香港身份證／護照上顯示之姓名；
b) 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
c) 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。

3.1.1.4 電子證書（保密）

透過證書上的主體名稱（於**附錄 B** 內指明）可識別電子證書（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） 登記人機構授權單位名稱。

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電子證書（機構）或電子證書（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

電子證書（個人）及電子證書（保密）一律只用英文發出。如電子證書（保密）之登記人機構僅有中文名稱或僅提供其中文名稱，該電子證書將不會顯示其機構名稱。

電子證書（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，該電子證書將會包含其機構及分行中文名稱。如電子證書（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***”。

3.1.2 名稱需有意義

根據本準則發出證書所採用主體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 登記人的匿名或假名

根據本準則香港郵政不會發出匿名或假名證書。

3.1.4 詮釋名稱規則

電子證書會載入之登記人名稱（主體名稱）類型見第 3.1.1 條。有關電子證書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。

3.1.6 商標的認可、驗證及角色

申請人及登記人向香港郵政保證（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。

香港郵政可酌情處理任何有關商標權、服務商標、網域名稱、商用名稱、公司名稱或任何其他知識產權擁爭議之事宜並享有最終決定權。

3.2 初始身分驗證

香港郵政會按照本準則，在發出任何電子證書前驗證申請人的身分及權限。

電子證書（個人）

電子證書（個人）的申請人必須到指定之香港郵政處所或其他香港郵政指定之機構處所，填妥並遞交一份香港郵政認可的申請表。

申請人須完成第 3.2.3 條所述身份驗證程序。完成身份驗證程序後，申請人會收到一個電子證書“密碼信封”。

電子證書（機構）及電子證書（保密）
電子證書（機構）及電子證書（保密）的機構申請人的身份認證將透過以下其中一個程序完成：

a) 申請人之獲授權代表須親身到指定之香港郵政處所或其他香港郵政指定之機構處所，遞交填妥及簽署的電子證書申請表及登記人協議書，並出示獲授權代表的香港身份證或護照以核實身份。該前述處所的人員會以面對面的方式，覆核並認證申請資料，隨後將申請轉交香港郵政核證機關處理。
b) 香港郵政可酌情容許申請人提交申請表連獲授權代表簽署的香港身份證或護照副本，或連獲授權代表的有效電子證書（機構）的有效數碼簽署，代替獲授權代表親身辦理手續，惟須符合（i）登記機構在過去提交的申請中已認證該獲授權代表的身分，以及該獲授權代表曾於該次申請時親身到指定的香港郵政處所或其他香港郵政指定之機構處所核實身分；及（ii）有合理理據再次確認獲授權代表的身分，例如經電話與他核實身分或核對他在過去提交的申請表上的簽署。
c) 香港郵政在有懷疑的情況下，可拒絕有關申請。

3.2.1 證明擁有私人密碼匙之方法
香港郵政為登記人提供代製密碼匙服務。香港郵政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。私人密碼匙連同證書將儲存在電子證書儲存媒體上，並以本準則第 4.1、4.2 及 4.3 條中指明的安全方式交付予登記人。

3.2.2 組織機構身分認證
就電子證書（機構）及電子證書（保密）而言，香港郵政會按照本核證作業準則的規定，透過文件證明及核實獲授權代表的身分，以核實登記人機構的身分及其存在。

每份電子證書（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（如適用）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電子證書（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；及
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。

每份電子證書（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（如適用）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
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。

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（如適用）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、撤銷及續發香港郵政電子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。

獲發出多於一年有效期電子證書（機構）或電子證書（保密）之登記人機構，香港郵政會約於電

子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，香港郵政可根據本準則第 4.9 條（證書撤銷及暫時吊銷）的條款暫時吊銷或撤銷發出予該登記人機構的證書。

3.2.3 個人身分認證

各電子證書（個人）申請人的身分認證將透過以下其中一個程序完成：

a) 各證書申請人須親身到指定之香港郵政處所或其他已獲香港郵政指定之機構處所，遞交填妥及簽署的電子證書申請表及登記人協議，並出示申請人香港身份證。該前述處所人員會以面對面的方式，覆核並認證申請資料，隨後將申請遞轉交香港郵政核證機關處理。
b) 各證書申請人須出示其有效電子證書（個人）的有效數碼簽署。並無持有有效電子證書（個人）之申請人應按上文（a）的程序核實身分。
c) 香港郵政在有懷疑的情況下，可拒絕有關申請。

3.2.4 沒有驗證的登記人資訊

香港郵政會按照本準則驗證載於電子證書內的主體資料。未按照本準則驗證的登記人資料，不得載於電子證書內。

3.2.5 權限及郵箱控制驗證

不適用。

3.2.6 互操作準則

香港郵政根據本準則而發出的電子證書，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。

3.3 密碼匙更新請求的標識與鑒別

香港郵政支援在證書滿前為現有證書提供密碼匙更新，以作以下兩種用途：

i） 更換證書，即在申請證書後更改了部分（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。

在上述兩種情況下，均須按照第 4.2.1 條的規定再次進行身分識別及身分認證。

3.3.1 常規密碼匙更新時的身分識別及身分認證

香港郵政不支援應登記人要求為更換證書而進行例行密碼匙更新。證書的密碼匙更新通常會作為證書續期程序的一部分進行，或由香港郵政酌情決定作為證書更換程序的一部分進行。

3.3.2 證書撤銷後密碼匙更新時的身分識別及身分認證

香港郵政不容許對已屆滿有效期或已撤銷的證書進行密碼匙更新。

登記人或登記人機構的獲授權代表，必須按照第 3.2 條所述重新辦理首次登記程序。

3.4 撤銷請求的身分識別及身分認證

香港郵政接到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）登記人在香港郵政網站內遞交有關要求的指定網頁完成身分認證後，於確認網頁上作出確認；(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，以及在電子證書被撤銷或有效期屆滿後申請新的電子證書，均須按照本核證作業準則第 3 及第 4 條所述程序遞交申請。

4.1.1 誰能遞交證書申請

符合資格的申請人可按照本核證作業準則的規定申請電子證書。就電子證書（機構）及電子證書（保密）而言，申請須由獲授權代表代表登記人機構遞交。

4.1.2 登記過程與責任

根據本核證作業準則發出的電子證書申請人必須完成登記程序，包括：

a) 填妥申請表並於指定香港郵政處所或香港郵政指定的其他機構的處所遞交；
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) 接受香港郵政代表申請人代製密碼匙，以產生私人密碼匙及相應的公開密碼匙。

電子證書申請表一經遞交，申請人即批准香港郵政向其他人士或在香港郵政儲存庫公布其電子證書，並接受香港郵政將發給申請人的電子證書。

4.2 處理證書申請

4.2.1 履行鑒別及認證職能

用以證明登記人機構及獲授權代表身分的文件，於本準則第 3.2.2 條及第 3.2.3 條說明。電子證書密碼信封將於獲授權代表在指定香港郵政處所遞交申請時當面接收，或於完成身分認證程序後，以安全方式交付予獲授權代表，例如掛號郵件。

電子證書（個人）

- **證書申請**

a) 根據本核證作業準則發出之電子證書（個人）的申請人，須於指定香港郵政處所或香港郵政指定的其他機構的處所用香港郵政指定的表格遞交申請。

b) 如不屬於電子證書（個人）“互認版”，申請人必須接受將電子證書及私人密碼匙儲存在作為電子證書儲存媒體的電子證書檔案 USB 上。

c) 如屬於電子證書（個人）“互認版”，申請人只可選擇指定的 PKCS#11 相容電子證書儲存媒體作為電子證書及私人密碼匙的儲存媒體。

d) 如不屬於電子證書（個人）“互認版”，申請人可於遞交電子證書申請表時，要求額外一份電子證書及私人密碼匙的副本，此副本可被逐一儲存於由申請人所提供的替代儲存媒體上。如香港郵政認為該要求可以接受，則此電子證書及私人密碼匙副本會被逐一儲存於替代儲存媒體上。在這種情況下，於（b）中所述程序適用於此電子證書及私人密碼

匙副本，尤其是此電子證書及私人密碼匙副本會受個人密碼所保護，並以安全方式交付予申請人。

e) 香港郵政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。

f) 電子證書申請表一經遞交，申請人即批准香港郵政向其他人士或在香港郵政儲存庫公布其電子證書，並接受香港郵政將發給申請人的電子證書。

- **核對身分**
  申請人須按照第 3.2.3 條完成身分認證程序。完成身分認證程序後，申請人會收到一個電子證書“密碼信封”。

- **郵箱授權驗證**
  不適用。

核實證書資料

申請人可瀏覽證書檔案或經香港郵政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郵政。

電子證書（機構）

- **證書申請**

a) 電子證書（機構）之申請人須到指定之香港郵政處所或其他香港郵政指定之機構處所遞交申請表格，包括按香港郵政要求之附加申請表格，連同申請書內列明的其他文件以及登記費用，一併交回。

b) 如不屬於電子證書（機構）“互認版”，申請人必需接受將電子證書及私人密碼匙儲存在作為電子證書儲存媒體的電子證書檔案 USB 上。

c) 申請人可於遞交電子證書申請表時，要求額外一份電子證書及私人密碼匙的副本，此副本可被逐一儲存於由申請人所提供的替代儲存媒體上。如香港郵政認為該要求可以接受，則此電子證書及私人密碼匙副本會被逐一儲存於替代儲存媒體上。在這種情況下，於（b）中所述程序適用於此電子證書及私人密碼匙副本，尤其是此電子證書及私人密碼匙副本會受電子證書個人密碼所保護，並以安全方式交付予申請人。

然而，如屬於電子證書（機構）“互認版”，申請人只可選擇指定的 PKCS#11 相容電子證書儲存媒體作為電子證書及私人密碼匙的儲存媒體。

d) 香港郵政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。

e) 電子證書申請表一經遞交，申請人即批准香港郵政向其他人士或在香港郵政儲存庫公布其電子證書，並接受香港郵政將發給申請人的電子證書。

- **核對身分**
  用以證明登記人機構、獲授權代表及授權用戶身分之文件，於本準則第 3.2.2 及 3.2.3 條

說明。電子證書”密碼信封”將於獲授權代表在指定之香港郵政處所提交申請表時當面接收， 或於完成核對身分手續後，以安全方式交付予獲授權代表，例如掛號郵件。

- **郵箱授權驗證**
  不適用。

電子證書（保密）

- **證書申請**

a) 電子證書（保密）之申請人須到指定之香港郵政處所或其他香港郵政指定之機構處所遞交申請。

b) 在申請電子證書時，申請人必需接受將電子證書及私人密碼匙儲存在作為電子證書儲存媒體的電子證書檔案 USB 上。

c) 申請人可於遞交電子證書申請表時，要求額外一份電子證書及私人密碼匙的副本，此副本可被逐一儲存於由申請人所提供的替代儲存媒體上。如香港郵政認為該要求可以接受，則此電子證書及私人密碼匙副本會被逐一儲存於替代儲存媒體上。在這種情況下，於（b）中所述程序適用於此電子證書及私人密碼匙副本，尤其是此電子證書及私人密碼匙副本會受電子證書個人密碼所保護，並以安全方式交付予申請人。

d) 電子證書申請表一經遞交，申請人即批准香港郵政向其他人士或在香港郵政儲存庫公布其電子證書，並接受香港郵政將發給申請人的電子證書。

- **核對身分**
  用以證明登記人機構及獲授權代表之文件，於本準則第 3.2.2 及 3.2.3 條說明。電子證書“密碼信封”將於獲授權代表在指定之香港郵政處所提交申請表時當面接收，或於完成核對身分手續後，以安全方式交付予獲授權代表，例如掛號郵件。

- **郵箱授權驗證**
  不適用。

- **公布電子證書**

  根據《電子交易條例》的規定，香港郵政會盡快在儲存庫公布已獲接受並已發出的電子證書（見第 2 條）。申請人可瀏覽證書檔案或經香港郵政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郵政。

4.2.2 證書申請批准和拒絕

完成身分認證程序後，香港郵政有義務通知申請人其申請獲接納或被拒絕。申請被拒絕的申請人隨後可重新申請。香港郵政有絕對酌情權保留拒絕申請的權力，且無須對因拒絕而產生的任何損失或費用承擔任何責任。

4.2.3 證書申請的處理期限

香港郵政將作出合理努力，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，香港郵政將盡合理努力完成證書申請時間如下：

證書類別	完成證書申請時間
電子證書（個人）	三個工作天
電子證書（個人）“互認版”	
電子證書（機構）	十個工作天
電子證書（機構）“互認版”	
電子證書（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 4.2.3 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郵政系統的香港郵政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，香港郵政批准其電子證書的申請。

電子證書（個人）

a) 在核對身分手續後，香港郵政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；
b) 以密碼保護的私人密碼匙及電子證書將隨後被儲存在申請人所選擇的電子證書儲存媒體及替代儲存媒體（若有的話）上。電子證書儲存媒體及替代儲存媒體（若有的話）會密封於一可防止改動的封套或其他容器內；並以安全方式交付予申請人，例如掛號郵件；
c) 申請人同意，一旦接獲電子證書儲存媒體及替代儲存媒體（若有的話），即須完全為私人密碼匙的安全保管負責，並同意將對由於任何情形引起的私人密碼匙外洩所造成的任何後果負責；
d) 所有存於香港郵政系統內的私人密碼匙均經加密。香港郵政會以恰當的保安措施防範私人密碼匙在未經授權下被接達或披露。在完成送遞電子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郵政系統中刪除。

電子證書（機構）／電子證書（保密）

e) 在核對身分手續後，香港郵政會在其處所內之穩當系統及環境下產生授權單位之電子證書（包括配對密碼匙），以保證私人密碼匙不受干擾；
f) 以密碼保護的私人密碼匙及電子證書將隨後被儲存在申請人所選擇的電子證書儲存媒體及替代儲存媒體（若有的話）上。電子證書儲存媒體及替代儲存媒體（若有的話）會密封於一可防止改動的封套或其他容器內；並以安全方式交付予獲授權代表，例如掛號郵件；
g) 申請人機構同意，他們一旦接獲電子證書儲存媒體及替代儲存媒體（若有的話），即須完全為私人密碼匙的安全保管負責，並同意他們將對由於任何情形引起私人密碼匙外洩所造成的任何後果負責。
h) 所有存於香港郵政系統內的私人密碼匙均經加密。香港郵政會以恰當的保安措施防範私人密碼匙在未經授權下被接達或披露。在完成送遞電子證書及私人密碼匙給獲授權代表後，申請人的私人密碼匙會從香港郵政系統中刪除。

4.3.2 電子認證服務機構和註冊機構對登記人的通告
完成身分認證程序後，香港郵政會透過登記人在申請過程中指定的電郵地址，以電郵通知申請人其申請獲得批准。

4.4 證書接受

4.4.1 構成接受證書的行為
申請人須於香港郵政網站 http://www.eCert.gov.hk 的指定網頁核實及確認電子證書所載資料的準確性。如申請人拒絕接受電子證書，香港郵政會撤銷該電子證書。登記人一旦使用電子證書，即視作已接受該電子證書。

申請人可瀏覽證書檔案或經香港郵政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郵政。

4.4.2 核證機關對證書的發布
所有已獲接受並發出的電子證書均會根據《電子交易條例》的規定在香港郵政儲存庫公布。

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
登記人必須按照本核證作業準則及證書所允許的用途使用電子證書及相應的私人密碼匙。

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，立即向香港郵政呈報丟失或外洩（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) 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。

電子證書（保密）的登記人亦有責任確保：

a) 獲授權使用者已獲登記人機構授權，並實際按照本核證作業準則，使用其證書及相關數碼簽署而不作任何其他用途；
b) 按照本核證作業準則用於透過加密及解密保護資料；
c) 不會試圖使用電子證書（保密）產生數碼簽署；及
d) 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。

4.5.2 倚據人士公開密碼匙和證書的使用
倚據電子證書的倚據人士須負責：

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。
c) 於倚據證書前查核證書撤銷清單上之證書狀態。
d) 如屬於電子證書（個人）“互認版”及電子證書（機構）“互認版”，於倚據前查閱廣東省經濟和信息化委員會公布的正式信任清單，以確認有關證書類別是否具有有效互認狀態及其有效期。有關資料亦載於數字政策辦公室備存的信任清單內，以供參考（見第 2.2.1 條）。
e) 執行所有適當證書路徑認可程序。
f) 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

電子證書可於證書有效期屆滿前續期，但須符合本核證作業準則的規定。

4.6.2 誰能要求證書續期

電子證書不會自動續期。若香港郵政接收到續期申請，即會根據第 3.2.2 及 3.2.3 條所述“機構申請人身分認證“及“個人身分認證“之過程進行認證。機構的獲授權代表或登記人須填妥證書續期申請表（可於香港郵政網址 http://www.eCert.gov.hk 下載），並連同申請表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）及 3.2.3（a）條中所述，新的獲授權代表亦須填妥申請表，一併交回。

4.6.3 證書續期請求的處理

4.6.3.1 電子證書（個人）續期

4.6.3.1.1 香港郵政會於證書的有效期即將屆滿前，向電子證書（個人）登記人發出有效期到期通知。證書可因應登記人的要求及香港郵政的酌情權，在證書的有效期屆滿前獲得續期。香港郵政不會為過期或已撤銷的證書續期。因應香港郵政的酌情權，發出給登記人的新證書的實際有效期會超過於下文所列的預設證書有效期：

如屬於電子證書（個人）“互認版”／電子證書（個人）（非互認版）：

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	新的電子證書的有效期可超過一年，但不會超過一年另一個月

4.6.3.1.2 透過上文 3.2.3（b）提及的有效數碼簽署為電子證書（個人）續期，可無需如首次申請般進行認證登記人身分的程序。登記人亦可填妥並簽署證書續期表格送交香港郵政申請續期。續期申請的詳情可向郵政局查詢或參閱香港郵政網址 http://www.eCert.gov.hk。證書一經續期，登記人的新配對密碼匙會透過香港郵政的代製密碼匙服務來產生。證書續期以後，只要登記人協議原有之條款及條件與續期當日有效的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之證書。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。

4.6.3.2 電子證書（機構）／電子證書（保密）續期

4.6.3.2.1　香港郵政會於證書的有效期即將屆滿前，向電子證書（機構）及電子證書（保密）登記人發出有效期到期通知。證書可因應登記人的要求及香港郵政的酌情權，在證書的有效期屆滿前獲得續期。香港郵政不會為過期或已撤銷的證書續期。因應香港郵政的酌情權，發出給登記人的新證書的實際有效期會超過證書的有效期：

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
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	新的電子證書的有效期可超過一年，但不會超過一年另一個月

4.6.3.2.2　電子證書（機構）及電子證書（保密）不會自動續期。若香港郵政接收到續期申請，即會根據第 3.2.2 條所述“機構申請人身分認證“程序進行認證。機構的獲授權代表須填妥證書續期申請表（可於香港郵政網址 http://www.eCert.gov.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 條所述，新的獲授權代表須填妥申請表，一併交回香港郵政。

4.6.3.2.3　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。

4.6.4　發出新證書時對登記人的通告
向登記人發出關於證書續期的通知與本準則第 4.3.2 條中所述有關新電子證書的方法相同。

4.6.5　構成接受續期證書的行為
登記人構成接受續期電子證書的行為，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布
香港郵政發布續期電子證書的方式，與本準則第 4.4.2 條中所描述的方法相同。

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郵政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
香港郵政只會接受來自同一登記人有關電子證書更換密碼匙的請求，或酌情處理。然而，香港郵政不會自動為電子證書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
證書密碼匙更新要求的處理程序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
香港郵政將通過本準則第 4.3.2 條中所述的方式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 條中所列的相同。

4.7.6 核證機關對密碼匙更新證書的發布
香港郵政發布密碼匙更新證書的方式與本準則第 4.4.2 條中所述的方法相同。

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電子證書。

4.8.1 證書變更的情形
不適用。

4.8.2 請求證書變更的實體
不適用。

4.8.3 證書變更請求的處理
不適用。

4.8.4 發出新證書時對登記人的通告
不適用。

4.8.5 構成接受變更證書的行為
不適用。

4.8.6 核證機關對變更證書的發佈
不適用。

4.8.7 核證機關對其他實體的通告
不適用。

4.9 證書撤銷和暫時吊銷

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。

4.9.1 證書撤銷的情形

4.9.1.1 若香港郵政私人密碼匙資料外洩，會導致香港郵政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，香港郵政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）。

4.9.1.2 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。

4.9.1.3 登記人之私人密碼匙或內載與某電子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，或電子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，向香港郵政申請撤銷證書。

4.9.1.4 不論何時，若有以下情況，香港郵政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電子證書（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電子證書（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電子證書（機構）或電子證書（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。

4.9.1.5 香港郵政會於下列任何事件發生後 24 小時內撤銷電子證書：

1) 香港郵政收到登記人以書面提出撤銷電子證書要求當日後的下一個工作日；
2) 香港郵政收到登記人通知，表示原來的證書申請未經授權，且登記人不會追溯給予有關授權當日後的下一個工作日；
3) 香港郵政取得證據，證明與電子證書內公開密碼匙相對應的登記人私人密碼匙已遭外洩；或
4) 香港郵政認為已經證明或證實有方法，可藉著電子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）。

4.9.1.6 香港郵政可於下列任何事件發生後 24 小時內撤銷電子證書，並且在任何情況下最遲會於 5 日內撤銷電子證書：

1) 香港郵政取得證據，顯示電子證書被不正當使用；
2) 香港郵政得悉登記人違反登記人協議中一項或多項條款列明之責任；
3) 香港郵政得悉電子證書所載資料有重大變更；
4) 香港郵政得悉電子證書並非按照香港郵政證書政策及／或核證作業準則發出；
5) 香港郵政確定或得悉電子證書所載任何資料並不準確；
6) 香港郵政發出電子證書的權利屆滿、被撤銷或終止，除非香港郵政已作出安排繼續維持證書撤銷清單儲存庫；
7) 香港郵政證書政策及／或核證作業準則規定必須撤銷證書；或
8) 香港郵政得悉存在已被證實或已獲證明的方法，會導致登記人的私人密碼匙遭受外洩，或有明確證據顯示用以產生私人密碼匙的特定方法存在缺陷。

4.9.1.7 香港郵政將嚴格控制，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。

4.9.2 誰能要求證書撤銷

登記人或登記人機構的獲授權代表，可透過傳真、郵寄、電郵（電郵地址載於 https://www.ecert.gov.hk/about/contact/index.html）、親身前往郵局或透過香港郵政網站 http://www.eCert.gov.hk 的指定網頁，向香港郵政提出撤銷證書要求。此外，登記人、倚據人士、應用程式軟件供應商及其他第三方亦可向香港郵政提交證書問題報告以通知香港郵政撤銷電子證書的合理原因。證書問題報告必須指明要求撤銷的登記人或登記人機構，並須指明有證據支持的撤銷原因。香港郵政可在沒有及不作事先通知之情況下撤銷證書。

4.9.3 撤銷請求的程序

登記人，或登記人機構的獲授權代表，可透過香港郵政於 http://www.ecert.gov.hk/的指定網頁、傳真、郵寄、電郵（電郵地址載於 https://www.ecert.gov.hk/about/contact/index.html）或親身前往郵局，向香港郵政提出撤銷證書要求。如登記人未能繳付登記費及拒絕接受香港郵政的推廣活動以延長登記使用期，登記人須提出撤銷證書的要求。

香港郵政收到撤銷證書要求後，將核證該請求並核實撤銷的原因。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郵政網站的指定網頁上進行身分認證；（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。

香港郵政會按照本準則所載程序，通過更新證書撤銷清單以及透過電子郵件（如有聯繫電郵地址）通知登記人撤銷證書（ “撤銷通知書” ）。撤銷證書申請表格可從網站 http://www.eCert.gov.hk 下載。

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）。

香港郵政核證機關處理以傳真、郵寄、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　：　上午九時至中午十二時
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要求。如在該日早上六時或以前信號除下，處理撤銷證書要求會於上述辦公時間恢復；如信號在早上六時至十時正之間除下，處理撤銷證書要求將於該日（週六、週日或公眾假期除外）下午二時恢復。如信號在上午十時後除下，處理撤銷證書要求將於下一個工作日的辦公時間（週六、週日或公眾假期除外）恢復。

4.9.4　撤銷請求寬限期

撤銷要求寬限期（“寬限期”）指登記人必須在其進行撤銷要求的期間。登記人之私人密碼匙或內載與某電子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，或電子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，向香港郵政申請撤銷證書。

在登記人明知香港郵政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郵政，香港郵政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，則香港郵政毋須就任何該等交易向登記人或倚據人士承擔責任。

此外，登記人明知香港郵政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郵政擬撤銷證書時，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（由香港郵政或經登記人申請），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，則香港郵政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。

除非香港郵政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，香港郵政無須就香港郵政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。

4.9.5　核證機關處理撤銷請求的時限

透過香港郵政網站的指定網頁遞交撤銷證書要求後，有關撤銷狀態將於 24 小時內反映於證書撤銷清單。至於以其他方式提出的撤銷要求，香港郵政將盡合理努力，確保於以下日期的下一個工作日起計 24 小時內，把撤銷資料刊載於證書撤銷清單：（1）收到登記人的撤銷證書要求或撤銷證書的最終確認；或（2）在未有收到該等要求的情況下，香港郵政決定撤銷證書之日。然而，香港郵政不會於每次撤銷證書後立即更新及公布供公眾查閱的證書撤銷清單。只有在下一次證書撤銷清單更新及公布時，證書的已撤銷狀態才會反映於證書撤銷清單內。證書撤銷清單每日公布三次，並最少保存七年。

香港郵政會盡合理努力，在撤銷證書後 24 小時內，透過更新證書撤銷清單的方式及電子郵件（如有電子郵件地址）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

倚據人士在倚據本證書前，有負責於倚據證書前查核證書撤銷清單上之證書狀態。

利用由香港郵政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。

有關香港郵政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 證書撤銷清單發布頻率

當電子證書被撤銷時，香港郵政會適時發布有關信息（包括證書撤銷清單，如香港郵政授權撤銷清單（ARL）。

證書撤銷清單（CRL）及香港郵政授權撤銷清單（ARL）會按照附錄 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郵政網頁 http://www.eCert.gov.hk 發布。

4.9.8 發佈證書撤銷清單的最大滯後時間

香港郵政不採用證書撤銷清單的最大滯後時間。一般而言，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

香港郵政現時不會就按照本準則發出的電子證書提供線上證書狀態應答（OCSP）服務。

4.9.10 線上撤銷查詢規定

倚據人士必須在倚據證書之前，按照第 4.9.6 條確認證書的有效性。

4.9.11 撤銷公告的其他發布形式

不適用。

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（包括但不限於倚據人士及應用程式軟件供應商），可以透過香港郵政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”為理由告知香港郵政。如果香港郵政發現或懷疑有私人密碼匙資料被外洩，將盡商業上合理的努力通知登記人，並在發現該等撤銷原因後或按照本準則第 7.2（a）條之要求將證書撤銷清單內的撤銷原因代碼更新為“密碼匙外洩”。

透過密碼匙外洩報告網頁向香港郵政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“香港郵政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郵政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

香港郵政可在第 4.9.1.4 條所列情況下暫時吊銷證書，並會按照本準則所載程序，透過更新證書撤銷清單及電子郵件（如有聯絡電郵地址）通知登記人有關暫時吊銷（“撤銷通知書”）。

4.9.14 誰能要求暫時吊銷證書

登記人或登記人機構的獲授權代表，可透過傳真、郵寄、電郵、親身遞交或透過香港郵政網站

http://www.eCert.gov.hk 的指定網頁向香港郵政提出撤銷證書要求。

4.9.15 要求暫時吊銷的程序
按照第 4.9.3 條，如香港郵政未收到登記人的撤銷證書最終確認，證書將維持暫時吊銷狀態，並一直列載於證書撤銷清單內，直至證書屆滿。香港郵政可考慮登記人恢復已暫時吊銷證書有效性的要求。然而，恢復已暫時吊銷證書的有效性完全由香港郵政酌情決定。

所有已暫時吊銷或已撤銷證書的資料（包括用以識別證書暫時吊銷及撤銷原因的代碼），均會載於證書撤銷清單內（見第 7.2 條）。

證書暫時吊銷會以“certificateHold”原因代碼列載於證書撤銷清單內。

由“暫時吊銷”狀態恢復有效的證書，將不會載於其後發布的證書撤銷清單內。

4.9.16 暫時吊銷的期限限制
證書暫時吊銷可持續至證書有效期屆滿為止。

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，包括表明撤銷證書的原因代碼將刊載於證書撤銷清單內（見第 7.2 條）。

4.10.2 服務可用性
證書狀態服務 24x7 保持開放。

4.10.3 運作特點
不適用。

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，證書被香港郵政撤銷；
b) 在證書登記使用期到期前提出終止服務的申請，並獲香港郵政接受；
c) 證書登記使用期滿，沒有進行證書更新或密碼匙更新。

香港郵政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 密碼匙托管與復原

4.12.1 密碼匙託管與復原的策略及實施
香港郵政使用之電子證書系統並無為香港郵政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 工作階段密碼匙封裝及復原政策與實施

不適用。

5· 設施、管理和運作控制

5.1 實體控制

5.1.1 選址及建造
香港郵政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，香港郵政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
香港郵政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，香港郵政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郵政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郵政控制之權標），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。印刷文件包括登記人協議及身分確認文件之影印本由香港郵政、承辦商或其核證登記機關妥為保存。獲授權人員方可以取閱該等紀錄。

5.1.7 廢物處理
香港郵政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
香港郵政已建立關鍵系統（包括香港郵政核證系統）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（包括進入香港郵政核證機關資料庫之受限制運作）之香港郵政、承辦商或代表香港郵政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郵政核證機關運作之行政人員。

5.2.2 每項任務需要的人數
香港郵政私人密碼匙儲存在可防止篡改加密硬件裝置內。香港郵政採用多人式控制（3 選 2 多人控制）啟動、使用、終止香港郵政私人密碼匙。

5.2.3 每個角色的鑑別及認證
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 需要職責分割的角色
香港郵政已為所有涉及香港郵政電子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、經驗和無過失要求
香港郵政及承辦商採用之人員及管理政策可合理確保香港郵政、承辦商或代表香港郵政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
香港郵政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／或香港郵政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郵政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
香港郵政、承辦商及核證登記機關須盡合理努力確保其所有人員（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
香港郵政、承辦商及核證登記機關須盡合理努力，為其人員提供適當及充足的培訓（擔任核心

職位的人員每年至少接受一次培訓），以確保其有能力履行職責，以及有效推行及遵守保安政策。

5.3.5 工作崗位輪換週期和順序
不適用。

5.3.6 未授權行為的處罰
香港郵政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
獲被委派執行受信職務的承辦商人員應遵守第 5.3 條就該等職務所訂明的職責及要求，並受上文第 5.3.6 條處罰所約束。

5.3.8 向人員提供之文件
香港郵政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。

香港郵政、承辦商及核證登記機關之間傳送的所有文件及資料，均須按照香港郵政不時訂明的規程，以受控及安全的方式交付。

5.4 審計日誌程序

5.4.1 記錄事件類型
香港郵政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：

核證機關證書及密碼匙生命周期事件，包括：
- 密碼匙的生成、備份、儲存、復原、存檔及銷毀；
- 證書的申請、續期、密碼匙更新要求及撤銷；
- 批准及拒絕證書申請；
- 加密硬件裝置生命週期管理事件；
- 產生證書撤銷清單；及
- 推出新的證書結構及停用現有證書結構。

登記人證書生命週期管理事件，包括：

- 證書的申請、續期、密碼匙更新要求及撤銷；
- 本準則規定的所有驗證行為；
- 批准及拒絕證書申請；
- 證書簽發；及
- 產生證書撤銷清單。

保安事件，包括：

- 成功及不成功的公匙基建系統存取嘗試；
- 已執行的公匙基建及保安系統操作；
- 保安設定檔變更；
- 在證書系統上安裝、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。

日誌記錄必須包括下列資料：

a) 事件發生的日期及時間；
b) 作出日誌記錄的人員身分；及
c) 事件描述。

5.4.2 處理紀錄之次數
香港郵政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郵政核證機關的行動、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七年。

5.4.4 審核紀錄之保護
香港郵政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
香港郵政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）
香港郵政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
香港郵政擁有自動處理系統，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
脆弱性評估為香港郵政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
香港郵政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。香港郵政（或由其代表）存有以下數據：

a) 系統設備結構檔案
b) 評估結果及／或設備合格覆檢（如曾進行）
c) 核證作業準則及其修訂本或最新版本
d) 對香港郵政具約束力而構成合約之協議
e) 所有發出或公布之證書及證書撤銷清單
f) 定期事件紀錄
g) 其他需用以核實存檔內容之數據
h) 證書系統建設和升級文檔；
i) 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；
j) 審計記錄；
k) 員工資料，包括但不限於背景調查、錄用、培訓等資料；
l) 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 第 5.5.1 條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郵政視為適當之方式存放於系統內。

5.5.3 存檔保護
香港郵政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 電子郵戳的要求
存檔資料均註明開設存檔項目之時間及日期。香港郵政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）
存檔資料由香港郵政在內部收集。

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

5.6 密碼匙變更
由香港郵政產生，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）。香港郵政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郵政網頁 http://www.eCert.gov.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 事故和資料外洩處理程序
香港郵政備有事故處理程序，以指引人員應對保安事故、自然災害及其他可能導致系統受損的

類似事件。為維持證書服務的完整性，香港郵政制定、記錄及定期測試適當的應變及災難復原計劃和程序。

香港郵政備有全面而可行的大規模撤銷事件應變計劃，並每年對計劃進行測試，以及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，香港郵政將評估事件的影響，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，香港郵政根據本準則簽發電子證書的私人密碼匙資料外洩或遭破壞而無法復原，香港郵政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，香港郵政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，香港郵政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。

如根據本準則簽發電子證書的香港郵政私人密碼匙資料外洩，香港郵政會即時知會數字政策專員並作出公布。香港郵政的私人密碼匙資料一旦外洩，香港郵政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，香港郵政根據本準則簽發電子證書的私人密碼匙資料外洩或遭破壞而無法復原，香港郵政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郵政公開密碼匙及如何向登記人重新發出證書。香港郵政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 災難後的持續營運能力

香港郵政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郵政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，香港郵政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 核證機關或核證登記機關終止服務

如香港郵政停止擔任核證機關之職能，即按“香港郵政終止服務計劃”所定程序知會數字政策專員並作出公布。在終止服務後，香港郵政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，或其代表香港郵政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

本條說明香港郵政特別為保障加密密碼匙及相關數據所訂之技術措施。控制香港郵政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、使用及毀滅香港郵政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，否則香港郵政及申請人／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。香港郵政產生配對根源密碼匙，用以發出符合本準則之證書。倘若由香港郵政爲申請人代製密碼匙，在完成送遞電子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郵政系統中刪除。香港郵政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，香港郵政會：

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；及
c) 由合資格的審計人員提交報告，報告發表意見認為香港郵政在其密碼匙和電子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

香港郵政會代表申請人／登記人按照代製密碼匙的要求產生電子證書的配對密碼匙。

6.1.3 公開密碼匙交付予證書發出人

用於核證機關數碼簽署之各香港郵政配對密碼匙之公開密碼匙可從網站 http://www.eCert.gov.hk 取得。香港郵政採取保護措施，以防該等密碼匙被人更改。

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郵政配對密碼匙之公開密碼匙可從網站 http://www.eCert.gov.hk 取得。香港郵政採取保護措施，以防該等密碼匙被人更改。

6.1.5 密碼匙大小

香港郵政之簽署配對密碼匙為 2048 位元 RSA。登記人配對密碼匙為 2048 位元 RSA。

6.1.6 公開密碼匙參數的生成和品質檢查

香港郵政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）

電子證書之密碼匙只可用於電子證書結構及本準則容許的用途。如電子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，電子證書的數碼簽署只可用於提供身分認證、資料完整性及不可否認性。香港郵政根源密碼匙（用於製造或發出符合本準則證書之密碼匙）只用於簽署（a）證書及（b）證書撤銷清單。

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
香港郵政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
香港郵政私人密碼匙儲存在可防止篡改加密硬件裝置內。香港郵政採用多人式控制（3 選 2 多人控制）啟動、使用、終止香港郵政私人密碼匙。

6.2.3 私人密碼匙托管
香港郵政使用之電子證書系統並無為香港郵政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。有關香港郵政私人密碼匙的備存，見第 6.2.4 條。

6.2.4 私人密碼匙備存
香港郵政私人密碼匙的備存，是使用達到 FIPS 140-2 第 3 級保安標準的裝置加密及儲存。香港郵政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
所有私人密碼匙不會存檔。

6.2.6 私人密碼匙於密碼模組之間傳遞
當香港郵政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。另外香港郵政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
香港郵政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
香港郵政核證機關根源密碼匙使用期不超過 25 年（另見第 5.6 條）。所有香港郵政密碼匙之產生、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 5.5 條詳述香港郵政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。

香港郵政核證機關根源密碼匙使用期不超過 25 年（另見第 5.6 條）。所有香港郵政密碼匙之產生、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 5.5 條詳述香港郵政公開密碼匙紀錄存檔之工作。

6.3.2 證書操作期和配對密碼匙使用期限
香港郵政核證機關根源密碼匙使用期不超過 25 年（另見第 5.6 條）。所有香港郵政密碼匙之產生、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 5.5 條詳述香港郵政公開密碼匙紀錄存檔之工作。

證書的有效期由產生自香港郵政系統當日起即日生效。

根據本核證作業準則在登記使用期內而發出之證書有效期可不同於上述之有效期（見第 4.6 條）。電子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
香港郵政私人密碼匙儲存在可防止篡改加密硬件裝置內。香港郵政採用多人式控制（3 選 2 多人控制）啟動、使用、終止香港郵政私人密碼匙。

6.4.2 啟動數據的保護
香港郵政私人密碼匙儲存在可防止篡改加密硬件裝置內。香港郵政採用多人式控制（3 選 2 多人控制）啟動、使用、終止香港郵政私人密碼匙。

6.4.3 激活數據的其他範疇
不適用。

6.5 電腦保安控制

6.5.1 特定電腦保安技術要求
香港郵政實行多人控制措施，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）。香港郵政已制定保安程序，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 8 條遵守規定之評估。香港郵政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，香港郵政將盡合理努力，清除所有可能載有與電子證書服務保安有關資料的儲存內容，並加以確認。

6.5.2 電腦安全評估
不適用。

6.6 生命週期技術控制

6.6.1 系統開發控制

香港郵政制定控制程序，為香港郵政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。

6.6.2 保安管理控制

香港郵政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件變更的控制。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

不適用。

6.7 網絡保安控制

香港郵政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。

香港郵政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。香港郵政會進行風險評估，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，香港郵政會評估相關風險，並制訂及執行有記錄的緩解計劃。

6.8 電子郵戳

香港郵政使用網絡時間協定（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）。香港郵政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 D** 載有電子證書之特點摘要。

香港郵政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）的非連續電子證書序號。

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

香港郵政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電子證書的資訊。

當電子證書因下列其中一項原因被撤銷時，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** **（RFC 5280 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）
暫時吊銷	6 = 證書暫時吊銷（certificateHold）

以下說明香港郵政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”：

- 香港郵政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
- 香港郵政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
- 香港郵政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郵政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 條所述的香港郵政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，則香港郵政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” 理由要求香港郵政核證機關撤銷證書，並且沒有證明其以往或目前擁有證書的相關私人密碼匙，香港郵政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。

當香港郵政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，則香港郵政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，當香港郵政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”：

- 香港郵政核證機關得到證書被不正當使用的證據；或
- 香港郵政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
- 香港郵政核證機關得知證書中的所載資料有重大變動；或
- 香港郵政核證機關確定或得知證書中的任何資料並不準確；或
- 香港郵政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站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獲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
- 香港郵政核證機關得悉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稱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撤銷其證書；或
- 香港郵政核證機關收到可核實的證據，證明證書登記人已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，否則在下列情況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
- 香港郵政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
- 香港郵政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
- 香港郵政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
- 香港郵政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。

f) 撤銷理由識別碼（6）“證書暫時吊銷”

撤銷理由識別碼“證書暫時吊銷”旨在用於顯示以下情況：

- 證書登記人已要求暫時吊銷證書；或
- 香港郵政核證機關按照本準則第 4.9.13 條暫時吊銷證書。

否則，不得使用“證書暫時吊銷”撤銷理由識別碼。

有關證書撤銷清單結構詳情情見**附錄 C**。

7.2.1 版本編號

香港郵政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
不適用。

7.3.1 版本編號
不適用。

7.3.2 線上證書狀態應答延伸欄位
不適用。

8． 遵守規定審核和其他評估

香港郵政作為認可核證機關，須根據《條例》第 43（1）條編寫和提交評估報告。

8.1 評估的頻率及情形

遵守規定審核評估須至少每十二個月進行一次。

8.2 評估者的資格

獨立外部審計員進行合規評估所須具備的資歷，須符合《條例》及《認可核證機關業務守則》所訂明的要求。

8.3 評估者與被評估實體之間的關係

合規評估由獨立於香港郵政的外部審計員進行，有關審計員須符合《條例》及《認可核證機關業務守則》所訂明的要求。

8.4 評估內容

香港郵政就其發出、撤銷及公布電子證書的系統進行合規評估，以確定本核證作業準則是否獲妥善遵循。該等評估須按照《條例》及《認可核證機關業務守則》所訂明的要求進行。

8.5 對問題與不足採取的措施

如審計員在審核中發現不符合適用法律、本核證作業準則或與香港郵政服務有關的任何其他合約責任的重大情況，則：（1）審計員須記錄有關差異；（2）審計員須立即通知香港郵政；及（3）香港郵政須根據有關差異的性質及影響範圍，制定適當的糾正措施計劃以糾正有關不符合情況，並決定是否就已發出的政府電子證書採取任何補救措施。

8.6 評估結果的傳達與發布

核證機關的 WebTrust 審核報告會於 http://www.eCert.gov.hk/product/cps/ecert 供公眾查閱。根據《條例》第 43（1）條編製的合規評估報告，則會提交予數字政策專員。

8.7 自我審核

不適用。

9． 法律責任和其他業務條款

9.1 費用

9.1.1 證書簽發和續期費用

除獲得香港郵政豁免，否則一切登記及行政費用須於每一登記使用期開始前由電子證書登記人付清。香港郵政保留絕對權力，不時檢討及訂定登記及行政費的收費水平，並經其網址 http://www.eCert.gov.hk 通知登記人及公眾。根據香港郵政及翹晉電子商務有限公司之合約條款，翹晉電子商務有限公司可收取電子證書之登記年費、續期費用及行政費。

9.1.1.1 電子證書（個人）

每份電子證書（個人）（包括首次及續期申請）年費為 50 港元，承辦商就電子證書（個人）登記費用提供推廣折扣優惠，詳情請參閱香港郵政網址 http://www.eCert.gov.hk 或經由第 1.5.2 條所列之途徑向香港郵政核證機關作出查詢。每份電子證書會儲存在需另付費的電子證書檔案 USB 內，最新的電子證書檔案 USB 費用會在香港郵政網站 http://www.eCert.gov.hk 公布。

電子證書（個人）非“互認版”收費	**一年有效期的電子證書**
首次申請及續期	每份電子證書 港幣 50 元*
電子證書儲存媒體	每份電子證書會儲存在需另付費的電子證書檔案 USB 內，最新的電子證書檔案 USB 費用會在香港郵政網站 http://www.eCert.gov.hk 公布。

*承辦商就電子證書（個人）提供登記費推廣折扣優惠，詳情請參閱香港郵政網站 http://www.eCert.gov.hk。

每份電子證書（個人）“互認版”的付費如下：

電子證書（個人） “互認版”收費	**一年有效期的電子證書**
首次申請及續期	每份電子證書 港幣 50 元*
電子證書儲存媒體	每份電子證書可付費存放於指定之 PKCS#11 兼容的儲存媒體中，最新的儲存媒體費用會在香港郵政網頁 http://www.eCert.gov.hk 公佈。

9.1.1.2 電子證書（機構）

電子證書（機構）非“互認版”：

電子證書（機構）非“互認版”收費	一年有效期的電子證書
首次申請	每份電子證書 港幣 50 元
非首次申請或續期	每份電子證書 港幣 150 元
登記費	承辦商就電子證書（機構）非“互認版”登記費用提供推廣折扣優惠，詳情請參閱香港郵政網址 http://www.eCert.gov.hk 或經由第 1.5.2 條所列之途徑向香港郵政核證機關作出查詢。
行政費 （不論授權用戶數目多少）	每份申請港幣 150 元
電子證書儲存媒體	每份電子證書會儲存在需另付費的電子證書檔案 USB 內，最新的電子證書檔案 USB 費用會在香港郵政網站 http://www.eCert.gov.hk 公布。

電子證書（機構）“互認版”：

電子證書（機構）“互認版”收費	一年有效期的電子證書
新申請或續期	每份電子證書 港幣 50 元
行政費 （不論授權用戶數目多少）	每份申請港幣 150 元
電子證書儲存媒體	每份電子證書可付費存放於指定之 PKCS#11 兼容的儲存媒體中，最新的儲存媒體費用會在香港郵政網頁 http://www.eCert.gov.hk 公佈。

9.1.1.3 電子證書（保密）

電子證書（保密）收費	一年有效期的電子證書
新申請或續期	每份電子證書 港幣 150 元
行政費 （不論授權單位數目多少）	每份申請港幣 150 元
電子證書儲存媒體	每份電子證書會儲存在需另付費的電子證書檔案 USB 內，最新的電子證書檔案 USB 費用會在香港郵政網站 http://www.eCert.gov.hk 公布。

9.1.2 證書查詢費用

香港郵政可對直接進入其證書資料庫收取合理費用。

9.1.3 證書撤銷或狀態資訊的查詢費用

香港郵政不會收取撤銷證書費用，亦不會對使用證書撤銷清單查閱已發出證書的有效性收取費用。

9.1.4 其他服務費用

香港郵政會不時檢討。

9.1.5 退款政策

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郵政，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，則香港郵政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郵政，則費用不會自動退還，而由香港郵政酌情退回。

9.2 財務責任

9.2.1 保險範圍

香港郵政維持專業責任／錯誤及遺漏保險，保額不少於一百萬美元。此外，該保險亦涵蓋根據《電子交易條例》條文就證書所訂倚據限額而可能產生或實際產生的責任及申索。

9.2.2 其他資產

不適用。

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電子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；但登記人及其授權用戶或授權單位的名稱（如適用），以及香港郵政或承辦商在履行本準則下香港郵政責任所必需的其他資料除外。

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。已發布的證書及撤銷資料被視為公共資訊。

9.3.3 保護機密資料的責任

在履行與香港郵政發出、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郵政、承辦商、核證登記機關及任何香港郵政分包商之人員，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。香港郵政會確保香港郵政、承辦商、核證登記機關及任何香港郵政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，不得將包括上文第 9.3.1 條所述的資料對外發布。除非法庭發出傳票或命令，或香港法例另有規定，香港郵政尤其不得發表登記人清單或其資料，惟無法追溯個別登記人之綜合資料除外。

9.4 個人資料私隱

9.4.1 私隱方案
香港郵政已實施符合本核證作業準則的私隱政策。香港郵政的私隱政策於香港郵政網站 http://www.eCert.gov.hk 公布。

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

9.4.3 不被視作私隱資料
已發布的證書及撤銷資料均被視作公開資料。證書狀態資料及任何證書內容均視作非私隱資料。

9.4.4 保護私隱的責任
在履行與香港郵政發出、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郵政、承辦商、核證登記機關及任何香港郵政分包商之人員，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。香港郵政會確保香港郵政、承辦商、核證登記機關及任何香港郵政分包商之人員均會依循此條限制事項。

9.4.5 使用私隱資料的通告與同意
作為根據本準則申請電子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；香港郵政或承辦商需根據本準則履行其責任之情況除外。

9.4.6 根據法律或行政程序作出的披露
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，不得將包括上文第 9.3.1 條所述的資料對外發布。除非法庭發出傳票或命令，或香港法例另有規定，香港郵政尤其不得發表登記人清單或其資料，惟無法追溯個別登記人之綜合資料除外。

9.4.7 其他資料披露情況
不適用。

9.5 知識產權
香港郵政擁有與其資料庫、網站、電子證書、商標及香港郵政發布的任何其他刊物（包括本核證作業準則）有關的一切知識產權。

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郵政所有，日後亦然。

9.6 陳述及擔保

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，香港郵政發布在其儲存庫中（見第 2 條）。

根據本準則而發出之證書，香港郵政向根據本準則第 9.6.4 條及其他有關章條之倚據人士表明，香港郵政已根據本準則發出證書。透過公布本準則所述之證書，香港郵政即向根據本準則第 9.6.4 條及其他有關章條之倚據人士表明，香港郵政已根據本準則（包括第 3.2 條）所述的核查程序，以驗證證書持有人即為證書中的登記人（對於電子證書（個人））；以及該證書的簽發方確實是登記人機構（對於電子證書（機構）和電子證書（保密））。

除非獲得香港郵政授權，香港郵政署、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郵政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

核證登記機關遵照與香港郵政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）之條款對香港郵政負責。核證登記機關代表香港郵政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。除因疏忽、超越授權範圍行事、欺詐、刑事行為或其他類似因素的情況外，香港郵政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郵政的功能、權力、權利和職責負責。

核證登記機關代表香港郵政履行其於此等事項下的義務及責任。核證登記機關有權代表香港郵政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）。

9.6.3 登記人的陳述與擔保

各申請人（申請電子證書，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，即表示其向香港郵政保證（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) 除電子證書（個人）登記人、電子證書（機構）的授權用戶或電子證書（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) 使用與登記人電子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) 電子證書只會用於第 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登記期屆滿。
c) 不時將授權代表的委任或任何資料變動立即通知香港郵政。
d) 將可能致使香港郵政根據本準則第 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郵政。

e) 在登記人明確知曉香港郵政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郵政知會，香港郵政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) 在明知香港郵政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郵政知會擬撤銷證書時，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（由香港郵政或經申請人或登記人申請），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) 承認知悉一經遞交電子證書申請表，即授權向其他人或在香港郵政儲存庫公布其電子證書。
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郵政及／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

倚據電子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。
c) 於倚據證書前在適用情況下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。

9.6.5 其他參與者的陳述與擔保

承辦商依據香港郵政及承辦商之合約條款，包括承辦商作為香港郵政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、推廣及維持香港郵政核證機關之系統及服務，而對香港郵政負責。除因疏忽、超出授權範圍行事、欺詐、刑事行為或其他類似因素的情況外，香港郵政會依然對承辦商在其執行或將會執行香港郵政之功能、權力、權利及職能之行為負責。

9.7 免責聲明

香港郵政謹此與各登記人協議，根據本準則香港郵政、承辦商及代表香港郵政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。香港郵政不向登記人或倚據人士承擔任何絕對義務。**香港郵政不保證香港郵政、承辦商或代表香港郵政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郵政、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，儘管香港郵政、承辦商或代表香港郵政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郵政、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。

即如香港郵政、承辦商或代表香港郵政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郵政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，香港郵政、郵政署、承辦商或代表香港郵政之核證登記機關概不負責。

亦即如在香港郵政（郵政署、承辦商或代表香港郵政之核證登記機關）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郵政不能控制之情況遭受不良影響，香港郵政、郵政署、承辦商或任何核證登記機關概不負責。香港郵政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。

香港郵政、承辦商或代表香港郵政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郵政、承辦商或代表香港郵政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，香港郵政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，以及（對於登記人而言）登記人協議中的相關規定。除因疏忽、欺詐、超出授權範圍行事或其他類似情形（統稱“例外情況”）外，核證登記機關或承辦商的一切作為及不作為均視作香港郵政的作為及不作為，免責聲明及倚據限額同樣適用於該等情況。即使在例外情況下，在法律允許的範圍內，香港郵政、核證登記機關及承辦商均應依據本 9.8 條規定的免責聲明及倚據限額。

若發生：

a) 香港郵政違反本準則或登記人協議；
b) 香港郵政違反任何謹慎職責－尤其當登記人或倚據人士、或其他人、或以其他任何方式，倚據或使用香港郵政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；
c) 因根據本準則及實務守則規定須由香港郵政確認，並且在該證書或存儲庫中被錯誤陳述的任何資訊而造成的損失

之情況下，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，**香港郵政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，香港郵政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，若發生：

a) 香港郵政違反本準則或登記人協議（僅適用於登記人）；
b) 香港郵政違反任何謹慎職責－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郵政根據公開密碼匙基礎建設而發出之任何證書時－應根據本準則、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；或
c) 因根據本準則及實務守則規定須由香港郵政確認，並且在該證書或存儲庫中被錯誤陳述的任何資訊而造成的損失

之情況下，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），香港郵政所負法律責任限制於且任何情況下每份電子證書不得超過 20 萬港元（不論是電子證書（個人）或電子證書（機構）或電子證書（保密），並且無論上述索賠、違約及／或損失的數量為何；對於簽發給 18 歲以下人士的每份電子證書（個人），賠償限額均為 0 港元（即香港郵政對此類證書不會承擔任何責任）。

任何登記人或倚據人士如欲向香港郵政提出索償，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。

承辦商、任何核證登記機關，以及香港郵政署、承辦商或任何核證登記機關的任何職員、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郵政承認，就登記人及倚據人士所知，香港郵政署、承辦商或任何核證登記機關或其各自之任何職員、僱員或代理人（就任何出於真誠、並與香港郵政履行本登記人協議或由香港郵政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，並向香港郵政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）、並與香港郵政履行本登記人協議或由香港郵政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，並承認香港郵政享有充分法律及經濟利益以保護香港郵政署及上述機構及個人免受此等法律行動。

任何個人傷亡之責任均不在本準則、登記人協議或香港郵政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。

如因倚據由香港郵政（或其代表香港郵政行事的承辦商）發出的證書所支援，而屬某登記人或任何聲稱代表該登記人行事的人士的虛假或偽造數碼簽署而引致任何損失，而香港郵政已符合《條例》及《認可核證機關業務守則》的規定，則香港郵政、承辦商及其各自的高級人員、僱員或代理人，均毋須就登記人及倚據人士所蒙受的任何損失或損害承擔責任，而由於上述免責聲明，在此等情況下適用於任何證書的倚據限額並無需要適用。

9.9 賠償

香港郵政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：

"香港郵政署職員及承辦商按香港郵政署長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電子證書的準則（可瀏覽 www.eCert.gov.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。

香港郵政署長（經香港郵政署、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，在適用情況下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。*

若儘管由香港郵政署長（或其代表行事的承辦商）簽發的證書所支持的訂戶虛假或偽造數字簽名而導致任何損失，並且該署長已就該證書遵守了條例及業務守則的相關規定，則在此情況下，香港郵政署長、香港郵政署承辦商及其各自職員、僱員或代理人均無需對倚據人士之任何損失或損害承擔任何責任；此外，鑑於上述免責聲明，該證書依據條例所適用的任何倚據限額也不再適用。

在符合本準則－包括本準則第 9.8 及 9.9 條－以及本證書所載各項規定與例外情況的前提下，若香港郵政違反了任何注意義務（特別是根據本準則或法律規定須盡到的合理技能與注意義務，和／或因倚據人士或任何其他人依賴或使用香港郵政在公開密碼匙基礎設施計劃下簽發的證書而可能對倚據人士負有的任何義務），或因依賴本準則及業務守則規定須由香港郵政確認、但卻在該證書或資料庫中被錯誤陳述的資訊而導致損失，香港郵政所負法律責任限制於且任何情況下每份電子證書不得超過 20 萬港元（不論是電子證書（個人）或電子證書（機構）或電子證書（保密），且無論上述索賠、違約及／或損失的數量為何；對於簽發給 18 歲以下人士的每份電子證書（個人），賠償限額均為 0 港元（即香港郵政對此類證書不會承擔任何責任）。

索賠時限

任何倚據人士如擬向香港郵政署長索賠，且該索償源起於或以任何方式與發出、撤銷、暫時吊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郵政署長、香港郵政署、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。”

9.10 有效期限與終止

9.10.1 有效期限
有關準則一經香港郵政在網站 http://www.eCert.gov.hk 或香港郵政儲存庫公布，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，香港郵政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
本核證作業準則（包括其所有修訂及增編）持續有效，直至被更新版本取代為止。

9.10.3 終止與保留效力
如香港郵政停止擔任核證機關之職能，即按“香港郵政終止服務計劃”所定程序知會數字政策專員並作出公布。在終止服務後，香港郵政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。

香港郵政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：

東九龍郵政信箱 68777 號香港郵政核證機關
電郵地址 ：enquiry@eCert.gov.hk

9.12 修訂

9.12.1 修訂程序
香港郵政批准更新其核證作業準則後，有關準則一經香港郵政在網站 http://www.eCert.gov.hk 或香港郵政儲存庫公布，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，或獲得香港郵政署長之明確書面同意。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、倚據人士及香港郵政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，香港郵政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郵政網站 http://www.eCert.gov.hk 或香港郵政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
香港郵政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
除下文第 9.15 條規限，香港郵政關於本準則範圍內之事宜之決定，在沒有明顯錯誤的情況下均為最終決定。如聲稱存在明顯錯誤，有關申索，請送交下列地址：

東九龍郵政信箱 68777 號香港郵政核證機關
電郵地址 ：enquiry@eCert.gov.hk

9.14 管轄法律
本準則受香港特別行政區法律規管。

9.15 符合適用法律規定

9.15.1 司法管轄權
任何一方（不論是香港郵政、登記人、倚據人士、承辦商或核證登記機關（各稱為一方））如因本核證作業準則而產生或與之相關的任何爭議或分歧，須首先按照當時有效的《香港特別行政區政府調解規則》進行調解。

如上述爭議或分歧未能透過調解解決，任何一方均可就該爭議或分歧提出訴訟。各方同意，香港法院對該爭議或分歧享有專有司法管轄權。

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（不可放棄權利）
香港郵政未有執行本核證作業準則的任何條文，並不構成放棄其於日後執行該條文或本核證作業準則任何其他條文的權利。任何放棄權利必須以書面作出並由香港郵政簽署，方為有效。

9.16.5 不可抗力
香港郵政如因任何適用法律、規例或命令的規定；民事、政府或軍事機關的行動；任何由其他人士營運而香港郵政無法控制的電力、通訊或其他系統故障；火災、水災或其他緊急情況；罷工；恐怖主義行為或戰爭；天災；或其他超出其合理控制範圍且並非因其過失或疏忽所引致的類似原因，而被阻止、禁止或延遲履行任何作為或規定，或未能履行任何作為或規定，香港郵政毋須承擔任何責任。

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郵政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，香港郵政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。香港郵政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，香港郵政須承擔第 9.8 條所載責任。另外，由香港郵政轉讓的物品可內載其他與完成及接受電子證書無關之資料。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（非香港特別行政區政府各政策局及部門）自然人或法人並已申請電子證書。

“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郵政根源證書。

“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。

“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**“電子證書”**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。

“密碼匙外洩報告網頁”是香港郵政核證機關網站上的一個網頁，用於向香港郵政報告與證書相關的懷疑私人密碼匙資料外洩。

“合約”指香港郵政所批出之香港郵政核證機關的外判合約，以委任承辦商於 2023 年 7 月 1 日至 2026 年 6 月 30 日期間根據本作業準則營運及維持香港郵政核證機關之服務及系統。該合約年期已延長至 2027 年 6 月 30 日（包括當日）。

“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）。其為香港郵政根據認可核證機關

業務守則第 3.2 段所委任之代理人，根據合約條款，為香港郵政營運及維持香港郵政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 條下頒布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（包括其分支機構、承辦商、代表、繼任者或委託人）。

“電子證書檔案 USB” 為一種 USB 快閃記憶體，是儲存電子證書的儲存媒體。最新的電子證書檔案 USB 價格會在香港郵政網頁 http://www.eCert.gov.hk 公布。

“電子證書儲存媒體”指一種儲存媒體，例如電子證書檔案 USB，用於儲存電子證書及私人密碼匙。

“電子證書（個人）”，**“電子證書（機構）”**，**“電子證書（保密）”**可簡稱為證書或電子證書。

“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。

“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。

“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。

“香港”指中華人民共和國香港特別行政區。

“註冊機關”就電子證書而言：

(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。

“稅務局參考編號” 指稅務局向《稅務條例》（第 112 章）所指的申報財務機構／申報實體／第 4AA 部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／第 4AA 部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。

“互認證書策略” 指香港與廣東省兩地政府頒佈的《粵港兩地電子簽名證書互認辦法》下的《粵港電子簽名證書互認證書策略》。

“互認版”就一張電子證書（個人）或電子證書（機構）而言，指該證書符合香港與廣東省兩地政府頒佈的《粵港電子簽名證書互認證書策略》，使證書可用於粵港兩地跨境應用。

“OCSP”指線上證書狀態應答。

“線上證書狀態應答”指一種線上證書核對規約，允許倚據人士查明電子證書的狀態。

“條例”指香港法例第 553 章《電子交易條例》。

“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），除可儲存電子證書及支援加密功能外，亦符合由 RSA 實驗室公佈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。

“個人密碼”指用於保護授權用戶的電子證書及其私人密碼匙的密碼。

“香港郵政署長”指香港法例第 98 章《郵政署條例》所指署長。

“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。

“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/）。

“核證登記機關”指由香港郵政指定，代表香港郵政核證機關行使一定職能，並提供香港郵政核證機關之若干服務之機構。

“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。

“倚據人士”指加密之信息和／或數碼簽署之信息的接收方，其中寄件者是電子證書的持有人；或發送加密之信息和／或數碼簽署之信息，而接收者是電子證書的持有人。

“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。

“SSL” 指安全通訊端層（Secure Sockets Layer）的縮寫。

“中繼證書”指由香港郵政根源證書所簽發的中繼核證機關證書“Hongkong Post Root CA 2”，並用於簽發香港郵政認可證書。

“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（或獲發給證書的機構）；
(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”** 指由登記人及香港郵政（即香港郵政署長，代表香港政府）訂立的協議，該協議包括電子證書（個人）的登記人條款及條件，以及電子證書（機構）或電子證書（保密）的登記人條款及條件及本核證作業準則。如登記人為香港特別行政區政府各政策局或部門，則協議為諒解備忘錄而不具法律約束力。

“**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電子證書之機構。

“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。

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 - 香港郵政電子證書格式

本附錄詳述由中繼證書“Hongkong Post e-Cert CA 2 - 15”及“Hongkong Post e-Cert CA 2 - 17”根據本核證作業準則簽發的電子證書格式。如欲了解由香港郵政其他中繼證書或根據其他核證作業準則簽發的電子證書格式，請根據電子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) 電子證書（個人）格式

1.1 根源證書 “Hongkong Post Root CA 2” 之下

以下為適用於由中繼證書"Hongkong Post e-Cert CA 2 - 17”發出的電子證書（個人）:-

欄位名稱		**欄位內容**	
		電子證書（個人）	**發出予未滿18歲人仕的電子證書（個人）**
標準欄 (Standard fields)			
版本 (Version)		X.509 V3	
序號 (Serial number)		[由香港郵政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=Hongkong Post Root CA 2 -17 o=Hongkong Post l=Hong Kong s=Hong Kong c=HK	
有效期 (Validity period)	**不早於 (Not before)**	[由香港郵政系統設置的UTC 時間]	
	不遲於 (Not after)	[由香港郵政系統設置的UTC 時間]	
主體名稱 (Subject name)		cn=[申請人姓名]（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=Hongkong Post e-Cert (Personal) c=HK	cn=[申請人姓名]（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=Hongkong Post e-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=Hongkong Post Root CA 2 o=Hongkong Post 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	
		電子證書（個人）	發出予未滿18歲人仕的電子證書（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 policies)		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, Adobe Authentic Documents Trust	
證書撤銷清單分發點 (CRL distribution points)		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"Hongkong Post e-Cert CA 2 - 15”發出的電子證書（個人）“互認版”:-

欄位名稱		欄位內容
標準欄 (Standard fields)		
版本 (Version)		X.509 V3
序號 (Serial number)		[由香港郵政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=Hongkong Post Root CA 2 -15 o=Hongkong Post l=Hong Kong s=Hong Kong c=HK
有效期 (Validity period)	不早於 (Not before)	[由香港郵政系統設置的UTC 時間]
	不遲於 (Not after)	[由香港郵政系統設置的UTC 時間]
主體名稱 (Subject name)		cn=[申請人姓名] （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=Hongkong Post e-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

欄位名稱		欄位內容
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=Hongkong Post Root CA 2 o=Hongkong Post 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 policies)		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 =2.16.344.8.2.2008.810.2.2018.1.1 （附註 7） Policy Qualifier Id = User Notice Qualifier : Notice Text=[身份審核方式編碼] （附註 8） Policy Qualifier Id = CPS Qualifier : [核證作業準則的 URL] Policy Identifier = 1.3.6.1.4.1.16030.1.4 （附註 9） Policy Qualifier Id = CPS Qualifier : [核證作業準則的URL]
主體別名 (Subject alternative name)	DNS	[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, Adobe Authentic Documents Trust
證書撤銷清單分發點 (CRL distribution points)		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
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. “e-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. 本欄已增加一個互認證書策略的物件識別碼，以識別符合互認證書策略而發出的證書。
8. 本欄已增加一個根據互認證書策略定義的身份審核方式編碼。如果此欄位不存在或沒有定義，則表示已使用面對面的身份審核方式（即根據互認證書策略代碼“A”所定義的身份審核方式）。
9. 本欄已增加一個支持 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：

    cert_hkid_hash = SHA-1 (RSA*privatekey, sha-1* (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** 則會在香港郵政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 **SHA-1 (RSA*privatekey, sha-1* (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.eCert.gov.hk/crl/eCertCA2-17CRL1<xxxxx>.crl，由中繼證書"Hongkong Post eCert CA2 - 17"所發出，其中 <xxxxx> 為 經香港郵政系統產生，包含 5 個數字或字符的字串。（就 2019 年 7 月 1 日之前發出的證書撤銷清單分發點 URL 為 http://crl1.hongkongpost.gov.hk/crl/eCertCA2-17CRL1_<xxxx>.crl）。香港郵政會公佈各“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佈。
12. 證書撤銷清單分發點 URL 為 http://crl1.eCert.gov.hk/crl/eCertCA2-15CRL1<xxxxx>.crl，由中繼證書"Hongkong Post eCert CA2 - 15"所發出，其中 <xxxxx> 為 經香港郵政系統產生，包含 5 個數字或字符的字串。（就 2019 年 7 月 1 日之前發出的證書撤銷清單分發點 URL 為 http://crl1.hongkongpost.gov.hk/crl/eCertCA2-15CRL1_<xxxx>.crl）。香港郵政會公佈各“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佈。

2) 電子證書（機構）格式

2.1 根源證書 “Hongkong Post Root CA 2” 之下

以下為適用於由中繼證書"Hongkong Post e-Cert CA 2 - 17”發出的電子證書（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)		[由香港郵政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=Hongkong Post Root CA 2 -17 o=Hongkong Post l=Hong Kong s=Hong Kong c=HK
有效期 (Validity period)	不早於 (Not before)	[由香港郵政系統設置的UTC 時間]
	不遲於 (Not after)	[由香港郵政系統設置的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=Hongkong Post e-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=Hongkong Post Root CA 2 o=Hongkong Post 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 policies)		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	[[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, Adobe Authentic Documents Trust
證書撤銷清單分發點 (CRL distribution points)		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 commen		未使用

以下為適用於由中繼證書"Hongkong Post e-Cert CA 2 - 15”發出的電子證書（機構）“互認版” :-

欄位名稱		**欄位內容**
標準欄 (Standard fields)		
版本 (Version)		X.509 V3
序號 (Serial number)		[由香港郵政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=Hongkong Post Root CA 2 -15 o=Hongkong Post l=Hong Kong s=Hong Kong c=HK
有效期 (Validity period)	**不早於 (Not before)**	[由香港郵政系統設置的UTC 時間]
	不遲於 (Not after)	[由香港郵政系統設置的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=Hongkong Post e-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=Hongkong Post Root CA 2 o=Hongkong Post 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 policies)		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 =2.16.344.8.2.2008.810.2.2018.1.1 (附註 8) Policy Qualifier Id = CPS Qualifier : [核證作業準則的 URL] Policy Identifier = 1.3.6.1.4.1.16030.1.4 (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, Adobe Authentic Documents Trust
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 commen		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 代表香港郵政）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郵政核實,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. 本欄已增加一個互認證書策略的物件識別碼，以識別符合互認證書策略而發出的證書。
9. 本欄已增加一個支持 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.eCert.gov.hk/crl/eCertCA2-17CRL2.crl，此為中繼證書"Hongkong Post e-Cert CA2 - 17"所發出的“分割式證書撤銷清單”。（就 2019 年 7 月 1 日之前發出的證書撤銷清單分發點 URL 為 http://crl1.hongkongpost.gov.hk/crl/eCertCA2-17CRL2.crl）。
12. 證書撤銷清單分發點 URL 為 http://crl1.eCert.gov.hk/crl/eCertCA2-15CRL2.crl，此為中繼證書"Hongkong Post e-Cert CA 2 - 15"所發出的“分割式證書撤銷清單”。（就 2019 年 7 月 1 日之前發出的證書撤銷清單分發點 URL 為 http://crl1.hongkongpost.gov.hk/crl/eCertCA2-15CRL2.crl）。

3) 電子證書（保密）格式

3.1 根源證書“Hongkong Post Root CA 2”之下

以下為適用於由中繼證書“Hongkong Post e-Cert CA 2 - 17”發出的電子證書（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)		[由香港郵政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=Hongkong Post e-Cert CA 2 - 17, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK
有效期 (Validity period)	**不早於 (Not before)**	[由香港郵政系統設置的UTC 時間]
	不遲於 (Not after)	[由香港郵政系統設置的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=Hongkong Post e-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=Hongkong Post Root CA 2 o=Hongkong Post 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 policies)		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
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

欄位名稱		欄位內容
延伸密碼匙使用方法 (Extended key usage)		SSL Client
證書撤銷清單分發點 (CRL distribution points)		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 commen		未使用

附註:

1. 登記人機構之授權單位名稱。
2. 獲授權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 代表香港郵政）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.eCert.gov.hk/crl/eCertCA2-17CRL2.crl，此為中繼證書"Hongkong Post e-CertCA 2 - 17"所發出的“分割式證書撤銷清單” 。（就 2019 年 7 月 1 日之前發出的證書撤銷清單分發點 URL 為 http://crl1.hongkongpost.gov.hk/crl/eCertCA2-17CRL2.crl)。

附錄 C - 香港郵政證書撤銷清單（CRL）及香港郵政授權撤銷清單（ARL）格式

本**附錄 C** 詳述有關由中繼證書"Hongkong Post e-Cert CA 2 - 15"及"Hongkong Post e-Cert CA 2 - 17"所發出的證書撤銷清單，以及由根源證書"Hongkong Post 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。

香港郵政每天三次更新及公佈下述的證書已暫時吊銷或撤銷清單（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電子證書的資訊：

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"Hongkong Post e-Cert CA 2 - 17"所發出電子證書（個人）：
http://crl1.eCert.gov.hk/crl/eCertCA2-17CRL1_<xxxxx>.crl
其中 <xxxxx> 為包含 5 個數字或字符的字串。（就 2019 年 7 月 1 日之前發出的證書撤銷清單分發點 URL 為 http://crl1.hongkongpost.gov.hk/crl/eCertCA2-17CRL1_<xxxxx>.crl）

ii. 由中繼證書"Hongkong Post e-Cert CA 2 - 15"所發出電子證書（個人）“互認版”：
http://crl1.eCert.gov.hk/crl/eCertCA2-15CRL1_<xxxxx>.crl
其中 <xxxxx> 為包含 5 個數字或字符的字串。（就 2019 年 7 月 1 日之前發出的證書撤銷清單分發點 URL 為 http://crl1.hongkongpost.gov.hk/crl/eCertCA2-15CRL1_<xxxxx>.crl）

iii. 由中繼證書"Hongkong Post e-Cert CA 2 - 17"所發出電子證書（機構）及電子證書（保密）：
http://crl1.eCert.gov.hk/crl/eCertCA2-17CRL2.crl。（就 2019 年 7 月 1 日之前發出的證書撤銷清單分發點 URL 為 http://crl1.hongkongpost.gov.hk/crl/eCertCA2-17CRL2.crl）

iv. 由中繼證書"Hongkong Post e-Cert CA 2 - 15"所發出電子證書（機構）“互認版”
http://crl1.eCert.gov.hk/crl/eCertCA2-15CRL2.crl。（就 2019 年 7 月 1 日之前發出的證書撤銷清單分發點 URL 為 http://crl1.hongkongpost.gov.hk/crl/eCertCA2-15CRL2.crl）

b) **“整體證書撤銷清單”（Full CRL）**包含分別由中繼證書"Hongkong Post e-Cert CA 2 - 15"，"Hongkong Post e-Cert CA 2 - 17"所發出的所有已暫時吊銷或撤銷證書的資料。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"Hongkong Post e-Cert CA 2 - 15"所發出的證書：
http://crl1.eCert.gov.hk/crl/eCertCA2-15CRL1.crl 或
ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post e-Cert CA 2 - 15 CRL1, o=Hongkong Post, c=HK)

ii. 由中繼證書"Hongkong Post e-Cert CA 2 - 17"所發出的證書：
http://crl1.eCert.gov.hk/crl/eCertCA2-17CRL1.crl 或
ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post e-Cert CA 2 - 17 CRL1, o=Hongkong Post, 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 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，香港郵政會於更新時間後，盡快將最新的證書撤銷清單公佈。在不能預見及有需要的情況下，香港郵政可不作事前通知而更改上述證書撤銷清單的更新及公佈的時序。香港郵政也會在有需要及不作事前通知的情況下，於香港郵政網頁 http://www.eCert.gov.hk 公佈補充證書撤銷清單。

香港郵政會更新及公佈授權撤銷清單，而清單內載有已暫時吊銷或已撤銷的中繼證書的資料。香港郵政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. 根源證書"Hongkong Post Root CA2"所簽發的中繼證書
http://crl1.eCert.gov.hk/crl/RootCA2ARL.crl 或
ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post Root CA 2, o=Hongkong Post, c=HK)

（I） 由中繼證書"Hongkong Post e-Cert CA 2 - 15"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)		cn=Hongkong Post e-Cert CA 2 - 15 o=Hongkong Post 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 3）				
機關密碼匙識別名稱 (Authority Key Identifier)	發出人 (Issuer)	cn=Hongkong Post Root CA 2 o=Hongkong Post l=Hong Kong s=Hong Kong c=HK		此欄提供有關資料以識別用作簽署證書撤銷清單的私人密碼匙的配對公開密碼匙。
	序號 (Serial number)	[發出人證書的序號]		此欄顯示發出人證書的序號
證書撤銷清單號碼 (CRL number)		[由核證系統產生 – 每張分割式證書撤銷清單都有各自的順序]		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]

（II） 由中繼證書"Hongkong Post e-Cert CA 2 - 17"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)		cn=Hongkong Post e-Cert CA 2 - 17 o=Hongkong Post 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 3）				
機關密碼匙識別名稱 (Authority Key Identifier)	發出人 (Issuer)	cn=Hongkong Post Root CA 2 o=Hongkong Post l=Hong Kong s=Hong Kong c=HK		此欄提供有關資料以識別用作簽署證書撤銷清單的私人密碼匙的配對公開密碼匙。
	序號 (Serial number)	[發出人證書的序號]		此欄顯示發出人證書的序號
證書撤銷清單號碼 (CRL number)		[由核證系統產生－每張分割式證書撤銷清單都有各自的順序]		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"Hongkong Post 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
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

標準欄位 (Standard fields)	子欄位 (Sub-fields)	授權撤銷清單欄位內容	備註
發出人 (Issuer)		cn=Hongkong Post Root CA 2 o=Hongkong Post 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)	**發出人 (Issuer)**	cn=Hongkong Post Root CA2 o=Hongkong Post l=Hong Kong s=Hong Kong c=HK	此欄提供有關資料以識別用作簽署授權撤銷清單的私人密碼匙的配對公開密碼匙。
	序號 (Serial number)	[發出人證書的序號]	此欄顯示發出人證書的序號
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. 有關電子證書的證書撤銷清單，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，6 = 證書暫時吊銷，9 = 特權被撤銷

   否則，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 = 未註明；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. 除非另外註明，否則所有欄位均將設定為“非關鍵”。

附錄 D - 香港郵政電子證書 – 服務摘要

1) 電子證書（個人）

要點	電子證書（個人）	電子證書（個人） "互認版"	發出予未滿 18 歲人仕的 電子證書（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	由香港郵政代製產生		
核對身分	當面核對申請人的身分，或由申請人提供可經其有效電子證書（個人）證明的數碼簽署		
證書用途	數碼簽署及數據加密	數碼簽署	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（由香港郵政核證機關系統產生）		
登記費用	（見本核證作業準則第 9.1.1 條）		
證書有效期	一年		
	（見本核證作業準則第 4.6.3.1 及 6.3.2 條）		

2) 電子證書（機構）及電子證書（保密）

要點	電子證書（機構）	電子證書（機構）“互認版”	電子證書（保密）
登記人	持有由香港特別行政區政府發出的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	由香港郵政代製產生		
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	數碼簽署	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（由香港郵政系統產生） ▪ 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（由香港郵政系統產生） ▪ 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 9.1.1 條）		
證書有效期	一年		
	（見本核證作業準則第 4.6.3.2 及 6.3.2 條）		

附註：

1. 持有由香港特別行政區政府稅務局發出的有效證明文件的《稅務條例》（第 112 章）所指的申報財務機構／申報實體／第 4AA 部實體，亦可以成為電子證書（機構）的登記人（但非成為電子證書（機構）“互認版”的登記人）（見第 1.2.3.2 條）。
2. 對於持有由香港特別行政區政府稅務局向《稅務條例》（第 112 章）所指的申報財務機構／申報實體／第 4AA 部實體發出的有效證明文件的機構，電子證書只會顯示其稅務局參考編號。

附錄 E - 香港郵政電子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，香港郵政電子證書並無指定之核證登記機關。

附錄 F - 香港郵政電子證書服務 - 翹晉電子商務有限公司之合約分判商名單（若有的話）

截至本核證作業準則生效日期，就此核證作業準則而言，香港郵政電子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

參考項目	香港郵政核證機關根源證書名稱	有效期	備註
1	Hongkong Post Root CA 2	2015年9月5日 至 2040年9月5日	此根源證書由 2015 年 9 月 5 日起開始發出中繼證書。
2	Hongkong Post e-Cert CA 2 – 15	2026年7月7日 至 2030年9月5日	此中繼證書由根源證書“Hongkong Post Root CA 2”不作密碼匙更新而重新發出，並由 2026 年 10 月 1 日起開始根據本核證作業準則發出電子證書給申請人。
3	Hongkong Post e-Cert CA 2 – 17	2026年9月23日 至 2032年8月12日	此中繼證書由根源證書“Hongkong Post Root CA 2”不作密碼匙更新而重新發出，並由 2026 年 10 月 1 日起開始根據本核證作業準則發出電子證書給申請人。

附錄 H - 香港郵政電子證書特定應用名單及相對應之特定應用編碼

特定倚據人士名稱	特定應用	證書類別	界定為證書主體別名 DNS 欄位的特定應用編碼
香港特別行政區政府稅務局	AEOI [附註 1]功能	電子證書(機構)(不包括電子證書(機構)“互認版”)	“IRD_AEOI”

附註:

1. AEOI 代表 "自動交換資料"