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
政府電子證書（個人）
政府電子證書（功能單位）

“具安全電子郵件功能”

核證作業準則

日期：二零二六年十一月一日
物件識別碼：1.3.6.1.4.1.16030.1.8.15

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 中央管理通訊系統 13
1.3.4 登記人 13
1.3.5 倚據證書人士 14
1.3.6 其他參與者 15
1.4 證書用途 15
1.4.1 證書的適用用途 15
1.4.2 證書的禁止用途 15
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 決定本核證作業準則是否符合證書政策的人員 16
1.5.4 核證作業準則的審批程序 16
1.6 定義和縮寫 16
2． 公開資料及儲存庫責任 17
2.1 儲存庫 17
2.2 認證資料公布 17
2.3 公布時間或頻率 17
2.4 儲存庫進入控制 17
3． 鑑別及認證 18
3.1 命名 18
3.1.1 名稱類型 18
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 19
3.1.6 商標的認可、驗證及角色 19
3.2 初始身分驗證 19
3.2.1 證明擁有私人密碼匙之方法 19
3.2.2 機構申請人身分認證 20
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 密碼匙更新時的身分識別及身分認證 21
3.3.2 證書撤銷後密碼匙更新時的身分識別及身分認證 21
3.4 撤銷請求的標識與鑒別 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 23
4.2.3 證書申請的處理期限 23
4.3. 證書簽發 23
4.4 證書接受 23
4.4.1 構成接受證書的行為 23
4.4.2 核證機關對證書的發布 23
4.4.3 核證機關對其他實體的通告 23
4.5 配對密碼匙和證書的使用 23
4.5.1 登記人私人密碼匙及證書用途 24
4.5.2 倚據人士公開密碼匙和證書的使用 24
4.6 證書續期 24
4.6.1 證書續期的情形 24
4.6.2 誰能要求證書續期 24
4.6.3 證書續期請求的處理 24
4.6.4 發出新證書時對登記人的通告 25
4.6.5 構成接受續期證書的行為 25
4.6.6 核證機關對續期證書的發布 25
4.6.7 核證機關對其他實體的通告 25
4.7 證書密碼匙更新 25
4.7.1 證書密碼匙更新的情形 25
4.7.2 誰能要求證書公開密碼匙更新 25
4.7.3 證書密碼匙更新請求的處理 25
4.7.4 發出新證書時對登記人的通告 25
4.7.5 構成接受密碼匙更新證書的行為 26
4.7.6 核證機關對密碼匙更新證書的發布 26
4.7.7 核證機關對其他實體的通告 26
4.8 證書變更 26
4.8.1 證書變更的情形 26
4.8.2 請求證書變更的實體 26
4.8.3 證書變更請求的處理 26
4.8.4 發出新證書時對登記人的通告 26
4.8.5 構成接受變更證書的行為 26
4.8.6 核證機關對變更證書的發布 26
4.8.7 核證機關對其他實體的通告 26
4.9 證書撤銷和暫時吊銷 26
4.9.1 證書撤銷的情形 26
4.9.2 誰能要求證書撤銷 28
4.9.3 撤銷請求的程序 28
4.9.4 撤銷請求寬限期 28

4.9.5 核證機關處理撤銷請求的時限 29
4.9.6 供倚據人士檢查證書撤銷的規定 29
4.9.7 證書撤銷清單發布頻率 29
4.9.8 發佈證書撤銷清單的最大滯後時間 29
4.9.9 線上撤銷/狀態查詢的可用性 29
4.9.10 線上撤銷查詢規定 30
4.9.11 撤銷公告的其他發布形式 30
4.9.12 密碼匙資料外洩的特殊規定 30
4.9.13 證書暫時吊銷的情形 30
4.9.14 誰能要求暫時吊銷證書 30
4.9.15 要求暫時吊銷的程序 30
4.9.16 暫時吊銷的期限限制 30
4.10 證書狀態服務 30
4.10.1 操作特徵 30
4.10.2 服務可用性 30
4.10.3 運作特點 30
4.11 登記使用期結束 31
4.12 密碼匙托管與復原 31
4.12.1 密碼匙託管與復原的策略及實施 31
4.12.2 工作階段密碼匙封裝及復原政策與實施 31
5． 設施、管理和運作控制 32
5.1 實體控制 32
5.1.1 選址及建造 32
5.1.2 實體訪問 32
5.1.3 電力及空調 32
5.1.4 水患 32
5.1.5 火災防護 32
5.1.6 媒體存儲 32
5.1.7 廢物處理 32
5.1.8 場外備存 32
5.2 程序控制 33
5.2.1 受信職責 33
5.2.2 每項任務需要的人數 33
5.2.3 每個角色的鑑別及認證 33
5.2.4 需要職責分割的角色 33
5.3 人員控制 33
5.3.1 資格、經驗和無過失要求 33
5.3.2 背景調查程序 33
5.3.3 培訓要求 33
5.3.4 再培訓週期和要求 33
5.3.5 工作崗位輪換週期和順序 34
5.3.6 未授權行為的處罰 34
5.3.7 獨立承辦商的要求 34
5.3.8 向人員提供之文件 34
5.4 審計日誌程序 34

5.4.1 記錄事件類型 34
5.4.2 處理紀錄之次數 35
5.4.3 審核紀錄之存留期間 35
5.4.4 審核紀錄之保護 35
5.4.5 審核紀錄備存程序 35
5.4.6 審核收集系統（內部對外部） 35
5.4.7 事件主體的通告 35
5.4.8 脆弱性評估 35
5.5 紀錄存檔 35
5.5.1 存檔紀錄類型 35
5.5.2 存檔保存期限 36
5.5.3 存檔保護 36
5.5.4 存檔備份程序 36
5.5.5 電子郵戳的要求 36
5.5.6 存檔收集系統（內部對外部） 36
5.5.7 獲取及驗證存檔資料的程序 36
5.6 密碼匙變更 36
5.7 資料外洩與災難復原 36
5.7.1 事故和外洩處理程序 36
5.7.2 計算機資源、軟件和／或數據的損壞 37
5.7.3 私人密碼匙資料外洩之程序 37
5.7.4 災難後的持續營運能力 37
5.8 核證機關或核證登記機關終止服務 38
6． 技術保安控制 39
6.1 密碼匙之產生及安裝 39
6.1.1 產生配對密碼匙 39
6.1.2 私人密碼匙交付予登記人 39
6.1.3 公開密碼匙交付予證書發出人 39
6.1.4 核證機關公開密碼匙交付予倚據人士 39
6.1.5 密碼匙大小 39
6.1.6 公開密碼匙參數的生成和品質檢查 39
6.1.7 密碼匙用途（按照 X.509 v3 密碼匙使用方法欄位） 39
6.2 私人密碼匙保護和加密模組控制 40
6.2.1 加密模組的標準和控制 40
6.2.2 私人密碼匙（m 選 n）多人式控制 40
6.2.3 私人密碼匙托管 40
6.2.4 私人密碼匙備存 40
6.2.5 私人密碼匙存檔 40
6.2.6 私人密碼匙於密碼模組之間傳遞 40
6.2.7 私人密碼匙在加密模組的存儲 40
6.2.8 啟動私人密碼匙的方法 40
6.2.9 解除私人密碼匙啟動狀態的方法 40
6.2.10 銷毀私人密碼匙的方法 40
6.2.11 加密模組的評估 40
6.3 配對密碼匙管理其他範疇 41

6.3.1 公開密碼匙存檔 41
6.3.2 證書操作期和配對密碼匙使用期限 41
6.4 啟動數據 41
6.4.1 啟動數據的產生和安裝 41
6.4.2 啟動數據的保護 41
6.4.3 啟動數據的其他範疇 41
6.5 電腦保安控制 41
6.5.1 特定電腦保安技術要求 41
6.5.2 電腦安全評估 41
6.6 生命週期技術控制 42
6.6.1 系統開發控制 42
6.6.2 保安管理控制 42
6.6.3 生命週期的保安控制 42
6.7 網絡保安控制 42
6.8 電子郵戳 42
7． 證書、證書撤銷清單及線上證書狀態應答結構 43
7.1 證書結構 43
7.1.1 版本編號 43
7.1.2 證書延伸欄位 43
7.1.3 算式物件識別碼 43
7.1.4 名稱格式 43
7.1.5 名稱限制 43
7.1.6 證書策略物件識別碼 43
7.1.7 策略限制延伸欄位使用的政策 43
7.1.8 策略限定資格的語法和語義的政策 43
7.1.9 關鍵證書策略延伸欄位的語義處理 43
7.2 證書撤銷清單結構 43
7.2.1 版本編號 46
7.2.2 證書撤銷清單及證書撤銷清單資料延伸欄位 46
7.3 線上證書狀態應答結構 46
7.3.1 版本編號 46
7.3.2 線上證書狀態應答延伸欄位 46
8． 認證機構審計和其他評估 48
8.1 評估的頻率及情形 48
8.2 評估者的資格 48
8.3 評估者與被評估實體之間的關係 48
8.4 評估內容 48
8.5 對問題與不足採取的措施 48
8.6 評估結果的傳達與發布 48
8.7 自我審核 48
9． 法律責任和其他業務條款 49
9.1 登記費用 49
9.1.1 證書發出或續期費用 49
9.1.2 證書查詢費用 49
9.1.3 證書撤銷或狀態資訊的查詢費用 49

9.1.4 其他服務費用 49
9.1.5 退款政策 49
9.2 財務責任 49
9.2.1 保險範圍 49
9.2.2 其他資產 49
9.2.3 對最終實體的保險或擔保 49
9.3 業務信息機密 49
9.3.1 機密資料範圍 50
9.3.2 不屬於機密的資料 50
9.3.3 保護機密資料的責任 50
9.4 個人資料私隱 50
9.4.1 私隱方案 50
9.4.2 視作隱私的資料 50
9.4.3 不被視作私隱資料 50
9.4.4 保護私隱的責任 50
9.4.5 使用私隱資料的通告與同意 50
9.4.6 根據法律或行政程序作出的披露 51
9.4.7 其他資料披露情況 51
9.5 知識產權 51
9.6 陳述及擔保 51
9.6.1 核證機關的陳述與擔保 51
9.6.2 核證登記機關的陳述與擔保 51
9.6.3 登記人的陳述與擔保 51
9.6.4 倚據人士的陳述與擔保 52
9.6.5 其他參與者的陳述與擔保 53
9.7 免責聲明 54
9.8 有限責任 54
9.9 賠償 56
9.10 有效期限與終止 57
9.10.1 有效期限 57
9.10.2 終止 57
9.10.3 終止與保留效力 57
9.11 參與人士的個別通告與通知 57
9.12 修訂 58
9.12.1 修訂程序 58
9.12.2 通知機制和期限 58
9.12.3 必須修改物件識別碼的情形 58
9.13 爭議處理 58
9.14 管轄法律 58
9.15 符合適用法律規定 58
9.15.1 司法管轄權 58
9.16 一般條款 59
9.16.1 完整協議 59
9.16.2 轉讓 59
9.16.3 分割性 59

9.16.4 執行（不可放棄權利） 59
9.16.5 不可抗力 59
9.17 其他條款 59
9.17.1 非商品供應 59
附錄 A - 詞彙 61
附錄 B - 香港郵政政府電子證書格式 65
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 69
附錄 D - 香港郵政政府電子證書 – 服務摘要 72
附錄 E - 香港郵政政府電子證書登記人機構／核證登記機關名單及中央管理通訊系統（若有的話） 73
附錄 F - 香港郵政政府電子證書服務 - 翹晉電子商務有限公司之合約分判商名單（若有的話）79
附錄 G - 核證機關根源證書的有效期 80
附錄 H - 香港郵政政府電子證書相對應之指定應用 81

©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，為支援香港特別行政區內安全電子交易及通訊，包括以安全／多用途互聯網郵件延伸功能（S/MIME）進行安全電子郵件通訊。

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 條下頒布之*《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安全電子郵件證書（即政府電子證書）均為條例下的認可證書，在本核證作業準則內稱為“證書”或“政府電子證書”。

本核證作業準則列明適用於香港郵政所發出政府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安全電子郵件（S/MIME）用途，並按照核證機關／瀏覽器論壇（CA / Browser Forum）的 S/MIME 基線要求（Baseline Requirements for S/MIME）發出。

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政府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政府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。

本核證作業準則之設計旨在符合下列規範最新版本的要求：
- 核證機關／瀏覽器論壇（CA / Browser Forum）發布有關發行和管理公開可信 S/MIME 證書的基線要求（“基線要求”）；
- WebTrust 核證機關原則及準則；
- WebTrust 核證機關原則及準則－S/MIME。

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。

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及保障電子郵件通訊安全。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及安全電子郵件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政府電子證書（個人）及政府電子證書（機構單位），香港郵政已指明為認可證書。**對登記人及倚據人士而言，根據該條例香港郵政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）。香港郵政已指定核證登記機關為其代理人之事實並無減輕香港郵政使用穩當系統之義務，亦無變更電子證書作為獲認可證書具有之特性。

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作業準則發出的政府電子證書所制訂的核證作業準則（“本準則”）。本文件自制訂以來曾作出以下修訂。

版本編號	修訂說明	生效日期
1（.14）	根據 RFC 3647 制訂首個適用於發出政府電子證書（個人）／政府電子證書（機構單位），用以取代現有（OID 1.3.6.1.4.1.16030.1.8.13）的核證作業準則。	2026 年 10 月 1 日

版本編號	修訂說明	生效日期
2（.15）	調整政府電子證書的最長有效期由兩年縮短至一年以提升安全性與可靠性。	2026 年 11 月 1 日

香港郵政已獲 Internet Assigned Numbers Authority （IANA） 分配私人企業號碼 （Private Enterprise Number） 16030 號。 **“1.3.6.1.4.1.16030.1.8.15”** 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）。所有符合 S/MIME 基線要求（Baseline Requirements for S/MIME）的證書，均會載有以下額外識別碼：

政府電子證書	政策物件識別碼（OID）
政府電子證書（個人）	2.23.140.1.5.3.3 （由核證機關／瀏覽器論壇（CA / Browser Forum）編配，適用於符合贊助機構驗證嚴格證書政策（Sponsor-validated Strict Certificate Policy）的證書）
政府電子證書（機構單位）	2.23.140.1.5.2.3 （由核證機關／瀏覽器論壇（CA / Browser Forum）編配，適用於符合機構驗證嚴格證書政策（Organization-validated Strict Certificate Policy）

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、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、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） 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 載有香港郵政政府電子證書核證登記機關清單（若有的話）。

1.3.3 中央管理通訊系統

數字政策辦公室轄下的中央管理通訊系統（以下簡稱“中央管理通訊系統”），是提供在**附錄 H** 內的各項指定應用，供香港特別行政區政府各政策局／部門／辦公室（“政策局／部門／辦公室”）使用。中央管理通訊系統將採用由香港郵政核證機關簽發 X.509 第三版本之新特別用途數碼證書，以處理限閱資料。

香港郵政透過中央管理通訊系統指定的提出要求者角色來處理政府電子證書的申請人或登記人之事宜。在這方面，中央管理通訊系統是政府電子證書申請人和登記人的代理人。

同時，中央管理通訊系統的業務管理人員角色由政策局／部門／辦公室指定來核實政府電子證書申請人的身份。在這方面，業務管理人員作為政府電子證書的核證登記機關（以下稱為“核證登記機關”）。

所有其他功能和義務，包括中央管理通訊系統因證書生命週期管理及使用政府電子證書時而引致需要履行的功能，不論指定應用的性質如何，中央管理通訊系統作為其登記人的委託人或代理人（但不作為香港郵政承辦商的分包商或香港郵政的代理人），其功能和義務均由中央管理通訊系統承擔。

1.3.4 登記人

本準則下的登記人為**附錄 E** 所列的政策局／部門／辦公室。於本準則內，登記人亦可稱為“申請人”、“登記人”、“登記人機構”或“政策局／部門／辦公室”。政府電子證書的實際用戶及與登記人相關的用戶，分為以下兩類。

1.3.4.1 與登記人相關的用戶類別

1.3.4.1.1 政府電子證書（個人）

政府電子證書（個人）是應代表政策局／部門／辦公室（即申請人及**附錄 E** 所列的“登記人機構”）行事的提出要求者之要求，發給中央管理通訊系統用戶；並識別已獲該登記人機構授權使用該政府電子證書（個人）私人密碼匙的中央管理通訊系統用戶。登記人機構必須先與香港郵政作出安排，香港郵政才可以為登記人機構發出政府電子證書（個人）。

中央管理通訊系統用戶包括：

a) 公務員及由政府直接聘用的合約僱員；
b) 代理／個體聘用合約僱員（包括 T 合約資訊科技人員）；
c) 根據上述（b）項以外的合約安排（例如外判合約）聘用的常駐人員。

根據本準則香港郵政僅發出證書予其證書申請已獲批准並已以適當形式確認接受登記人協議之登記人機構。

持有此類證書（政府電子證書（個人））的中央管理通訊平台用戶，可於中央管理通訊平台使用該證書作下列用途，惟有關電子訊息不得分類為機密電郵：

a) （作為發送人）利用證書附加密碼簽署，以對電子訊息作出數碼簽署；
b) （作為發送人）利用數碼封印方式防止電子訊息遭受篡改；
c) （作為接收者）允許發送人使用接收者的公開密碼匙加密電子訊息；
d) （作為接收者）當收到電子訊息時將其解密；及
e) （作為接收者）讓登記人／登記人機構透過發送附有數碼簽署的確認訊息，以確認接收者的身分及確認收妥經加密的電子訊息。

政府電子證書（個人）只可由中央管理通訊系統用戶用於**附錄 H** 內列出對應其登記人機構之指定應用。

登記人機構向香港郵政承諾，除了按**附錄H**內所指的指定應用作上述用途外，不會授權予中央管理通訊系統用戶使用政府電子證書（個人）於任何其他用途。

1.3.4.1.2 政府電子證書（功能單位）

政府電子證書（功能單位）是應代表政策局／部門／辦公室（即申請人及**附錄E**所列的“登記人機構”）行事的提出要求者之要求，發給中央管理通訊系統功能單位；並識別已獲該登記人機構正式授權使用該政府電子證書（功能單位）私人密碼匙的中央管理通訊系統功能單位。登記人機構必須先與香港郵政作出安排，香港郵政才可以為登記人機構發出政府電子證書（功能單位）。

政府電子證書（功能單位） 提供給政策局／部門／辦公室之下的功能單位使用。

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確定接受登記人協議之登記人機構。

此類型證書僅限在中央管理通訊系統中使用：

a) 利用證書附加密碼簽署，以對電子訊息作出數碼簽署；
b) 利用數碼封印方式防止電子訊息遭受篡改；
c) 對電子訊息作保密及解密；及
d) 讓登記人／登記人機構透過發送附有數碼簽署的確認訊息，以確認接收者的身分（功能單位身分）及確認收妥經加密的電子訊息。

政府電子證書（功能單位）只可由中央管理通訊系統功能單位用於 附錄 H 內列出對應其登記人機構之指定應用。

登記人機構向香港郵政承諾，除了按附錄H內所指的指定應用作上述用途以外，不會授權予中央管理通訊系統功能單位使用政府電子證書（功能單位）於任何其他用途。

1.3.5 倚據證書人士

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的政府電子證書。

1.3.6 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。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 載有香港郵政政府電子證書服務 - 翹晉電子商務有限公司之合約分判商名單。

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。

根據本準則發出的證書只可用於安全電子郵件通訊用途，包括對電子郵件作出數碼簽署及加密。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 證書的禁止用途

根據本準則發出的證書不得用於安全電子郵件通訊以外的用途，包括但不限於傳輸層保安（TLS）認證、程式碼簽署或非電子郵件文件簽署。

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 決定本核證作業準則是否符合證書政策的人員

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證書有關之其他資料。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

2.3 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政府電子證書（個人）及政府電子證書（功能單位）的申請人及登記人所適用的身分識別、身分認證及郵箱驗證要求。

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 政府電子證書（個人）

透過證書上的主體名稱（於**附錄 B** 內指明），可識別政府電子證書（個人）登記人之身分，該名稱由以下資料組成：

a) 中央管理通訊系統用戶所控制郵箱的電郵地址（載於主體別名（Subject Alternative Name）延伸欄位）；
b) 中央管理通訊系統用戶於其身份證明文件上顯示的姓名；及
c) 登記人機構在獲香港法例認可之有關香港政府部門之登記名稱；如登記人機構為香港特別行政區政府政策局、部門或辦公室，則為該政策局、部門或辦公室之正式名稱。

3.1.1.2 政府電子證書（功能單位）

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

a) 中央管理通訊系統用戶所控制郵箱的電郵地址（載於主體別名（Subject Alternative Name）延伸欄位）；
b) 登記人機構在獲香港法例認可之有關香港政府部門之登記名稱；如登記人機構為香港特別行政區政府政策局、部門或辦公室，則為該政策局、部門或辦公室之正式名稱。

3.1.1.3 中央管理通訊系統之提出要求者、業務管理人員、決策局／部門／辦公室管理人員

決策局／部門／辦公室指定的提出要求者、業務管理人員及決策局／部門／辦公室管理人員雖替登記人機構於中央管理通訊系統辦理政府電子證書之申請手續，然而政府電子證書並不會辨識此人員身分。

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、網域名稱、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

業務管理人員角色可以進一步根據本作業準則第 1.3.4.1 條中提到的不同人員類別再作定義，以處理不同的驗證要求：

人員類別	說明
公務員及由政府直接聘用的合約僱員	須由具有業務管理人員角色的中央管理通訊系統用戶為這類人員執行“認證”步驟。該用戶負責核對證書持有人的證明文件*，與政府保存的人事記錄是否一致。
代理／個體聘用合約僱員（包括 T 合約資訊科技人員）	須由具有業務管理人員角色的中央管理通訊系統用戶為這類人員執行“認證”步驟。該用戶負責核對證書持有人的證明文件*，與代理保存的聘用記錄或決策局／部門／辦公室保存的個體聘用合約記錄及相關文件是否一致。
合約安排聘用的常駐人員	須由具有業務管理人員角色的中央管理通訊系統用戶為這類人員執行“認證”步驟。該用戶負責核對證書持有人的證明文件*，與用於決策局／部門／辦公室跟外判商訂立業務關係的合約、協議、單據或其他種類之法律文件內保存之可以證明證書持有人身份之記錄是否一致。

*證明文件可以是香港身份證，護照或決策局／部門／辦公室用於認證身份的其他文件。

如有疑問，香港郵政可拒絕接受該政府電子證書申請。

3.2.1 證明擁有私人密碼匙之方法
中央管理通訊系統在其處所內的穩當的系統及環境下使用硬件安全模塊（HSM）為登記人提供製作密碼匙服務，以確保私人密碼匙不被篡改，及產生並傳送含公開密碼匙的「簽發證書要求」（CSR）至香港郵政。香港郵政會在其處所內產生證書。包含了申請人公開密碼匙的證書在發出後會以安全的方式發送給申請人。

3.2.2 機構申請人身分認證

登記人機構為香港特別行政區政府的政策局、部門或辦公室，其身分乃透過其作為政府認可機構的地位及參與中央管理通訊平台而獲確認。

政府電子證書的申請由登記人機構指定的獲授權角色透過中央管理通訊平台遞交。中央管理通訊平台的使用及獲授權角色的委任，以證明登記人機構的身分及權限。

香港郵政採用以下登記方案：

a) GOVHK：適用於政府實體。

3.2.3 個人身分認證

就政府電子證書（個人）而言，中央管理通訊平台倚賴相關登記人機構先行核實個別人士的身分，以及於中央管理通訊平台內委派獲授權用戶角色。

中央管理通訊平台用戶帳戶的使用及角色委派，以證明與政府電子證書（個人）相關聯的人士已通過登記人機構的身分認證。（BR 第 3.2.4.1（6） 節）

3.2.4 沒有驗證的登記人資訊

香港郵政會按照 S/MIME 基線要求（Baseline Requirements for S/MIME）核實主體欄位及主體別名延伸欄位中的郵箱欄位（Mailbox Field）。未按照 S/MIME 基線要求（Baseline Requirements for S/MIME）核實的申請人資料，不得載於政府電子證書內。

3.2.5 權限及郵箱控制驗證

在初始身分驗證過程中，香港郵政會採用以下驗證方法，確認與政府電子證書相關的郵箱地址的權限或控制權。：

a） 透過網域驗證郵箱權限（S/MIME BR 第 3.2.2.1 條）
香港郵政可透過驗證郵箱地址中網域部分的控制權，確認申請人或登記人機構已獲授權代表有關郵箱持有人行事。如採用網域驗證方式，香港郵政只會使用核證機關／瀏覽器論壇《TLS 伺服器證書基線要求》第 3.2.2.4.12 條所訂明的認可網域驗證方法。

就郵箱授權或控制權的驗證而言，任何重複使用的資料、文件或已完成的驗證，均須於發出政府電子證書前不超過 30 日內取得或完成。

3.2.6 互操作準則

香港郵政根據本準則而發出的政府電子證書，在所有情況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有效期屆滿前為現有證書進行密碼匙更新，以作以下兩種用途：

i） 更換證書：即申請後部分（或全部沒有）主體資料有所更改，而登記人可選擇（或不選擇）更改與新證書相關連的密碼匙；

ii） 證書續期：即登記人希望延長現有證書的有效期，並可同時更改與該證書相關連的密碼匙。

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

3.3.1 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。

透過提出要求者行事的登記人，必須按照第 3.2 條所述重新辦理首次登記程序。

3.4 撤銷請求的標識與鑒別

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可由中央管理通訊平台透過採用 TLS 協定的專用及安全網絡連線向香港郵政核證機關提交載有證書撤銷資料的系統介面檔案作出。

4． 證書生命週期操作要求

4.1 證書申請

所有首次申請，以及在政府電子證書被撤銷或有效期屆滿後申請新的政府電子證書，申請人均須透過中央管理通訊平台遞交申請。中央管理通訊平台會完成申請程序並將申請傳送至香港郵政。

4.1.1 誰能遞交證書申請

就政府電子證書（個人）及政府電子證書（功能單位）而言，申請須由提出要求者透過中央管理通訊平台代表申請人遞交。

4.1.2 登記過程與責任

政府電子證書申請人必須完成登記程序，包括：

a) 申請人透過中央管理通訊平台以電子方式提交政府電子證書申請，即授權香港郵政向任何人士或在香港郵政儲存庫公布其政府電子證書，並接受香港郵政向其發出政府電子證書。；
b) 繳交所需費用；
c) 產生私人密碼匙及公開密碼匙。

申請人透過中央管理通訊平台以電子方式提交政府電子證書申請，即授權香港郵政向任何人士或在香港郵政儲存庫公布其政府電子證書，並接受香港郵政向其發出政府電子證書。

4.2 處理證書申請

4.2.1 履行鑒別及認證職能

用以證明申請人身分的文件，於本準則第 3.2 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。

同時，香港郵政在發出政府電子證書前，會按照 RFC 9495 檢索及處理核證機關授權紀錄（Certification Authority Authorisation Record）（「CAA 紀錄」）。若 CAA 紀錄存在，但記錄並未將香港郵政之域名「eCert.gov.hk」或「hongkongpost.gov.hk」列入為獲授權證書發出人的域名，則其證書申請將不會被繼續處理。若擬載於證書內的域名並沒有 CAA 紀錄，則香港郵政認為申請人允許香港郵政為該域名簽發證書。

郵箱授權驗證

完成第 3.2 條所述的身分認證、權限及郵箱控制驗證後，香港郵政會按照本核證作業準則所訂明的程序處理證書申請。

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。

公布政府電子證書

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政府電子證書（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

不適用。

4.3. 證書簽發

4.3.1 在核對身分手續後，中央管理通訊系統會在其處所內之穩當系統及環境下以硬件安全模塊（HSM）為登記人提供代製密碼匙服務，以保證私人密碼匙不受干擾，並生產及傳送包含公開密碼匙的簽發證書要求（CSR）至香港郵政。香港郵政會在其處所內的穩當系統及環境下，產生各中央管理通訊系統用戶／中央管理通訊系統功能單位的政府電子證書（包含公開密碼匙）。

4.3.2 政府電子證書會以電子方式交付予中央管理通訊系統用戶／中央管理通訊系統功能單位。

4.3.3 中央管理通訊系統同意，一旦接獲政府電子證書，即須完全爲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泄密所造成的任何後果負責。

4.3.4 所有存於中央管理通訊系統處所內之穩當系統及環境下的硬件安全模塊（HSM）內的私人密碼匙均經加密。中央管理通訊系統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。

4.4 證書接受

4.4.1 構成接受證書的行為

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政府電子證書均會根據《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

不適用。

4.5 配對密碼匙和證書的使用

4.5.1 登記人私人密碼匙及證書用途

登記人必須按照本核證作業準則及核證機關／瀏覽器論壇（CA / Browser Forum）S/MIME 基線要求（Baseline Requirements for S/MIME），僅將政府電子證書及相應的私人密碼匙用於安全電子郵件（S/MIME）用途。

登記人機構負責：

a) 承認會履行義務，使用合理預防措施來保護其政府電子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) 發現其政府電子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) 用於身份鑒別的政府電子證書，其私人密碼匙只可以在證書有效期內使用。
d) 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，僅將證書及相關私人密碼匙用於安全電子郵件用途；
e) 此等證書只可用以按照核證機關／瀏覽器論壇（CA / Browser Forum）S/MIME 基線要求（Baseline Requirements for S/MIME），僅用於安全電子郵件通訊，包括電子郵件的加密及解密，以及電子郵件的數碼簽署（如適用）；
f) 不會試圖使用政府電子證書的私人密碼匙用於本核證作業準則所允許的安全電子郵件通訊以外的任何用途；及
g) 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

倚據政府電子證書的人士須負責：

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) 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

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

登記人機構的提出要求者須透過中央管理通訊系統以電子方式遞交證書續期申請，及繳付續期費用。若香港郵政接收到續期申請，即會根據第 3.2.3 條所述“個人身分認證“之過程進行認證，如同收到新申請一樣。

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，方可透過中央管理通訊系統遞交續期要求。

4.6.3 證書續期請求的處理

4.6.3.1 政府電子證書續期

根據本核證作業準則發出或續期的證書，其有效期不得超過核證機關／瀏覽器論壇（CA / Browser Forum）S/MIME 基線要求（Baseline Requirements for S/MIME）所容許的最長有效期。

4.6.3.1.1　中央管理通訊平台會於證書的有效期即將屆滿前，向政府電子證書登登記人發出續期通知。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。

政府電子證書（個人）的證書有效期為一年。政策局／部門／辦公室可根據業務需要為證書持有人選擇證書的有效期。

政府電子證書（功能單位）的證書有效期為一年。政策局／部門／辦公室可根據業務需要為證書持有人選擇證書的有效期。

證書續期以後，中央管理通訊平台會透過其中央密碼匙產生服務為登記人產生新的配對密碼匙。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 條中所述有關新政府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政府電子證書的行為，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

香港郵政發布續期政府電子證書的方式，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政府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政府電子證書。

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布
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。暫時吊銷證書並不適用。

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，或相關政府電子證書所對應的中央管理通訊平台用戶角色有所改變或失效**，各登記人**必須立即**按照本準則的撤銷程序，向其政策局／部門／辦公室申請撤銷證書。

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) 知道或有理由相信在政府電子證書上指明之中央管理通訊平台用戶已非登記人機構之中央管理通訊平台用戶；或
h） 知道或有理由相信在政府電子證書上指明之中央管理通訊平台用戶已不再擁有其於登記人機構內之角色。

4.9.1.5 香港郵政會於下列任何事件發生後 24 小時內撤銷政府電子證書：

1) 香港郵政收到登記人以書面提出撤銷政府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，證明與政府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；
4) 香港郵政認為已經證明或證實有方法，可藉著政府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）；
5) 香港郵政取得證據，證明政府電子證書內任何郵箱地址的網域授權或郵箱控制驗證結果不應被信賴。

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

1) 政府電子證書不再符合 S/MIME 基線要求（Baseline Requirements for S/MIME）第 6.1.5 及第 6.1.6 條的規定；
2) 香港郵政取得證據，顯示政府電子證書被不正當使用；
3) 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；
4) 香港郵政得悉有任何情況顯示政府電子證書內使用的電郵地址或完整網域名稱（Fully-Qualified Domain Name）已不再獲合法允許使用（例如法院或仲裁機構已撤銷使用有關電郵地址或網域名稱的權利、登記人所訂立的相關牌照或服務協議已終止，或帳戶持有人未能維持該電郵地址或網域名稱的有效狀態）；
5) 香港郵政得悉政府電子證書所載資料有重大變更；
6) 香港郵政得悉政府電子證書並非按照 S/MIME 基線要求（Baseline Requirements for

S/MIME）或香港郵政證書政策及／或核證作業準則發出；
7) 香港郵政確定或得悉政府電子證書所載任何資料並不準確；
8) 香港郵政根據 S/MIME 基線要求（Baseline Requirements for S/MIME）發出政府電子證書的權利已屆滿、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或線上證書狀態通訊規約儲存庫；
9) 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
10) 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該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

提出要求者須登錄中央管理通訊系統，在中央管理通訊系統中為政府電子證書（個人）申請人或政府電子證書（功能單位）的功能單位完成並遞交撤銷證書要求。

業務管理人員須登錄中央管理通訊系統，並於決策局／部門／辦公室設定的預定工作日內批准該要求。

4.9.3 撤銷請求的程序

中央管理通訊系統可提供應用程式接口（API），透過專用和安全連接網絡從政策局／部門／辦公室系統接收撤銷證書要求，其要求包括了提出要求者和業務管理人員處理撤銷證書申請的工作流程資料。中央管理通訊系統須對撤銷證書要求進行驗證，並按照中央管理通訊系統記錄對提出要求者和業務管理人員的工作流程進行權限查核。

中央管理通訊系統須預備一份系統界面檔案，該檔案包含了撤銷證書資料，並透過專用和安全連接網絡以 TLS 規約遞交給香港郵政核證機關。

香港郵政核證機關會撤銷證書，該證書撤銷後即會永久失效。所有已撤銷的證書之有關資料將刊載於證書撤銷清單內。香港郵政核證機關將按照時間表公布證書撤銷清單。

中央管理通訊系統會透過專用且安全的網絡以 TLS 規約從香港郵政核證機關接收包含撤銷證書結果的系統界面檔案。因此，中央管理通訊系統須停止使用該政府電子證書，並通知所有涉及撤銷請求的中央管理通訊系統用戶。

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）。

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政府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，或政府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

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站 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站遞交證據，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站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
政府電子證書不設暫時吊銷安排。

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政府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載於第 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政府電子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站 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政府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，中央管理通訊平台為登記人代製的私人密碼匙資料外洩或遭破壞而無法復原，香港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。

如根據本準則簽發政府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政府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

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。

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根源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

中央管理通訊平台會代表申請人／登記人按照代製密碼匙的要求產生政府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 4096 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）

政府電子證書之密碼匙只可用於加密電子通訊及列於第 1.3.4.1 條的其他用途。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，政府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 解除私人密碼匙啟動狀態的方法
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。

證書的有效期由發出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 啟動數據的其他範疇
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政府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** 載有政府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政府電子證書的資訊。

當政府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）

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某政府電子證書曾被用作認證具欺詐性及誤導性的下級完整網域名稱；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． 認證機構審計和其他評估

本核證作業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。WebTrust 審計員亦須符合 S/MIME 基線要求第 8.2 條的規定。

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

香港郵政每季最少進行一次自我審核，抽樣檢查自上次自我審核以來所發出的電子證書中最少百分之三的隨機樣本。電子證書的自我審核須按照核證機關／瀏覽器論壇（CA / Browser Forum）採納的指引進行。

9． 法律責任和其他業務條款

9.1 登記費用

9.1.1 證書發出或續期費用

除獲得香港郵政豁免，否則一切登記費用須由政府電子證書登記人付清。有關政府電子證書的收費詳情，請參閱**附錄 H**。香港郵政保留絕對權力，不時檢討及訂定登記費的收費水平，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向政府電子證書登記人收取**附錄 H** 所列的登記費。

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 業務信息機密

9.3.1 機密資料範圍
作為根據本準則申請政府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；但登記人名稱、中央管理通訊平台用戶名稱，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政府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 條所述的資料在內的機密資料對外發布。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，以驗證證書申請人確為證書內所識別之登記人機構。

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
各登記人機構（由提出要求者代表）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，登記人機構據此條款同意，登記人機構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) 使用與證書所載公開密碼匙相對應的私人密碼匙執行指定應用，即屬上文第 1.3.4.1.1 條所述隸屬登記人機構的中央管理通訊平台用戶的行為，或上文第 1.3.4.1.2 條所述功能單位的行為；且該證書已獲接受，並於整個有效期內維持正常運作；
b) 證書所載之所有資料及由登記人機構作出之陳述均屬真實。
c) 證書將只會用於符合本核證作業準則之認可及合法用途。
d) 登記人機構將確保證書只限用於**附錄 H** 所訂明的指定應用；
e) 登記人機構同意遵守本核證作業準則、香港郵政的其他協議及政策聲明所載的條款及條件；
f) 登記人機構已授權中央管理通訊平台於**附錄 H** 所訂明的指定應用中取用該證書的私人密碼匙；
g) 在證書發出、接受及整個證書有效期內所提供之所有資料，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) 不時將政府電子證書中央管理通訊平台用戶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) 承認知悉一經遞交政府電子證書申請表，即授權向其他人或在香港郵政儲存庫公布其政府電子證書，包括中央管理通訊平台用戶或登記人機構的名稱。
h) 用於身份鑒別的證書，其私人密碼匙只可以在政府電子證書有效期內使用。

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

倚據政府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。

9.6.5.1 中央管理通訊系統之義務

中央管理通訊系統負責：

a） 在中央管理通訊系統中為“提出要求者”的用戶角色作出定義，以便政策局／部門／辦公室可以指定人員作為“提出要求者”以代表中央管理通訊系統用戶（申請人）提出申請證書，證書續期或證書撤銷的要求；
b） 在中央管理通訊系統中為“業務管理人員”的用戶角色作出定義，以便政策局／部門／辦公室可以指定人員作為核證登記機關，驗證申請人的身份並於中央管理通訊系統中批准證書申請、續期和撤銷要求；
c） 確保中央管理通訊系統用戶不能同時擔任“業務管理人員”和“提出要求者”的角色，以達到職責分離的要求；
d） 定義和提供予中央管理通訊系統中的不同用戶角色（“提出要求者”，“業務管理人員”）的審批工作流程，以執行證書申請，續期和撤銷的相應任務（遞交要求，驗證和審批要求）；
e） 代表申請人向香港郵政產生並遞交「簽發證書要求」（Certificate Signing Request），當中包括於提交時與中央管理通訊系統所知悉有關中央管理通訊系統用戶或功能單位的資料相符的資料，以及申請人確認的登記人條款及條件；
f） 代表申請人接受香港郵政以安全的方式發出的政府電子證書；
g） 確保登記人配對密碼匙只會在中央管理通訊系統的硬體安全模組（“HSM”）內產生和儲存；
h） 確保妥善保管登記人的配對密碼匙；
i） 確保政府電子證書僅用於**附錄 H** 中所規定之指定應用；
j） 確保中央管理通訊平台用戶或功能單位不被允許使用政府電子證書於**附錄 H** 中規定之指定應用以外的其他用途；
k） 確保只有在政府電子證書中列明的中央管理通訊平台用戶和／或功能單位才能使用其私人密碼匙於有關的指定應用進行數碼簽署；
l） 在中央管理通訊平台用戶或功能單位被允許於指定應用中使用政府電子證書前，核實中央管理通訊平台用戶或功能單位的身份；
m） 分配獨特的身份號碼給中央管理通訊平台用戶，此號碼於遞交政府電子證書申請時用來引用中央管理通訊平台用戶資料, 其必須與中央管理通訊平台用戶的身份證明具有唯一的相關性；
n） 每次在指定應用中使用政府電子證書時，根據儲存庫和證書撤銷清單中顯示的資料確保該政府電子證書並未過期或未被撤銷。如果政府電子證書已過期或被撤銷，不會使用該政府電子證書進行或完成指定應用；

9.6.5.2 政策局／部門／辦公室之義務

政策局／部門／辦公室除作為登記人所須承擔的責任外，亦須負責：

a） 指定“業務管理人員”作為核證登記機關以驗證申請人的身份，並透過中央管理通訊系統中的“業務管理人員”批准證書申請，續期和撤銷要求；
b） 保存由“業務管理人員”角色用作核證申請人身份的文件證明；
c） 指定“提出要求者”代表申請人提出證書申請、續期或撤銷的要求；
d） 確保“提出要求者”妥善完成申請程序, 並代表申請人確認接受登記人條款及條件；
e） 確保政府電子證書正確使用於**附錄 H** 中所規定之指定應用；及
f） 確保“業務管理人員”在政策局／部門／辦公室預先訂明的工作天內完成批核證書撤銷要求。

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、超越授權範圍行事或其他類似情況（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（不論是政府電子證書（個人）或政府電子證書（功能單位），並且無論上述索賠、違約及／或損失的數量為何。

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政府電子證書的準則（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（不論是政府電子證書（個人）或政府電子證書（功能單位）），且無論上述索賠、違約及／或損失的數量為何。

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。登記人及倚據人士同意接受香港特別行政區法院的非專屬司法管轄權。

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政府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

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”指附錄 E 中所列，透過提出要求者行事的申請人機構。

“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。

“應用程式接口”指一種應用程式介面，用於定義中央管理通訊系統與特定政策局／部門／辦公室系統之間的交互作用。當政策局／部門／辦公室在其系統中管理使用者帳戶時，中央管理通訊系統可透過此應用程式接口從特定的政策局／部門／辦公室系統接收使用者帳戶資訊。

“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。

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

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

“業務管理人員”指中央管理通訊系統中的一種使用者角色，負責核實申請人的身分（即擔任核證登記機關的角色），並審核中央管理通訊系統中的證書申請、續期及撤銷請求。

“核證機關”指向他人（可以為另一核證機關）發出證書者。

“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**“政府電子證書”**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。

“提交簽發證書要求”指由中央管理通訊系統發送給香港郵政、包含登記人的公開密碼匙，旨在申請證書的訊息。

“中央管理通訊系統”指由數字政策辦公室管理和支援的、在**附錄 E** 中列出的集中式管理服務平台，該平台提供上文第 9.6.5.1 節所概述的功能。

“中央管理通訊系統用戶”指由數字政策辦公室提供帳戶、可登入中央管理通訊系統並存取各類指定應用的政策局／部門／辦公室使用者。

“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。

“指定應用”指在**附錄 H** 中列出的指定應用。

“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。

“政府電子證書（個人）”或“政府電子證書（功能單位）”指政府電子證書或證書。

“硬體安全模組”是指一種硬體安全設備，用於儲存和管理證書，並保護配對密碼匙，防止其被篡改、匯出或複製。

“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。

"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。

"郵箱欄位"在電子證書而言，指包含主體郵箱位址的字段，該位址透過 rfc822Name 或其他類型為 id-on-SmtpUTF8Mailbox 的 otherName 值儲存在 subjectAltName 延伸欄位。

"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，允許倚據人士查明政府電子證書的狀態。

"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。

"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。

"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（包括核實申請人身分）之機構。

"倚據限額"指就認可證書倚據而指明之金錢限額。

"倚據人士"指透過使用中央管理通訊系統，來驗證另一中央管理通訊系統用戶或功能單位的身份，並據此決定是否信任該用戶或功能單位的數位簽署資訊的登記人機構的中央管理通訊系統用戶或功能單位。

"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。

“提出要求者”指中央管理通訊系統中的一種使用者角色，負責代表登記人機構提出證書申請、證書續約及證書撤銷請求。

“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。

“角色”指登記人機構賦予中央管理通訊系統用戶的職能或職責。

“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。

“S/MIME” 指安全／多用途互聯網郵件延伸（Secure/Multipurpose Internet Mail Extensions）的縮寫。

“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”指登記人機構。

“**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，該協議包括政府電子證書的登記人條款及條件，以及本核證作業準則。此協議屬於諒解備忘錄性質，不具法律約束力。

“**登記人機構”**指**附錄 E** 所列的實體。

“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。

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

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 - 香港郵政政府電子證書格式

本附錄詳述由中繼證書“Hongkong Post g-Cert CA 2 - 26”根據本核證作業準則簽發的政府電子證書格式。

1） 政府電子證書（個人）格式

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 - 26 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=[中央管理通訊系統用戶姓名] （附註1） g=[中央管理通訊系統用戶名] sn=[中央管理通訊系統用戶姓氏] e=[電子郵箱地址] （附註2） ou=[登記人機構分行／部門名稱] o=Hong Kong SAR Government c=HK Object Identifier (2.5.4.5) SERIALNUMBER=[登記人參考編號] （附註3） Object Identifier (OID: 2.5.4.97)=GOVHK
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）		
機關信息訪問 (Authority Information Access)	核證機關發出人 (Certification Authority Issuer)	URL=http://www1.eCert.gov.hk/root/ecert_ca_2-26.crt
機關密碼匙識別名稱 (Authority Key Identifier)	KeyID	[發出人證書的主體密碼匙標識符]
發出人證書的主體密碼匙標識符 (Subject Key Identifier)		[由主體公開密碼匙衍生]
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） （附註4）		Policy Identifier = [本準則的物件識別碼] （附註 5） Policy Identifier = 2.23.140.1.5.3.3 （附註 6） Policy Identifier = 1.3.6.1.4.1.16030.1.10.4 （附註7）

欄位名稱		欄位內容
主體別名（Subject alternative name）	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）**	未使用
	路徑長度限制（Path length constraint）	未使用
延伸密碼匙使用方法（Extended key usage）		S/MIME
證書撤銷清單分發點（CRL distribution point）		分發點名稱 = [證書撤銷清單分發點URL]（附註8）

附註:

1. 中央管理通訊系統用戶格式：以英文格式 記載- 姓氏（大寫）+ 名（例如: CHAN Tai Man David）。
2. 登記人機構提供之中央管理通訊系統用戶電子郵箱地址。
3. 登記人參考編號：10 位數字。
4. 由中繼證書簽發的證書符合本準則、核證機關／瀏覽器論壇 S/MIME 基線要求。
5. 本欄已包括本核證作業準則的物件識別碼 (Object Identifier, OID)。請參閱本準則第 1.2 條。
6. 證書策略物件識別碼由核證機關／瀏覽器論壇分配給符合贊助機構驗證嚴格證書政策的電子證書。
7. 香港郵政分配物件識別碼顯示，其持有人是政府電子證書（個人）之登記人。
8. 證書撤銷清單分發點 URL 為 http://crl1.eCert.gov.hk/crl/eCertCA2-26CRL2.crl，此為中繼證書"Hongkong Post e-Cert CA 2 - 26"所發出的「整體證書撤銷清單」。

2） 政府電子證書（功能單位）格式

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 - 26 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=Hong Kong SAR Government e=[電子郵箱地址]（附註1） ou=[登記人機構分行／部門名稱] o=Hong Kong SAR Government c=HK Object Identifier (2.5.4.5) SERIALNUMBER=[登記人參考編號]（附註3） Object Identifier (OID: 2.5.4.97)=GOVHK
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）		
機關信息訪問 (Authority Information Access)	核證機關發出人 (Certification Authority Issuer)	URL=http://www1.eCert.gov.hk/root/ecert_ca_2-26.crt
機關密碼匙識別名稱 (Authority Key Identifier)	KeyID	[發出人證書的主體密碼匙標識符]
發出人證書的主體密碼匙標識符 (Subject Key Identifier)		[由主體公開密碼匙衍生]
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）（附註3）		Policy Identifier = [本準則的物件識別碼]（附註 4） Policy Identifier = 2.23.140.1.5.2.3（附註 5） Policy Identifier = 1.3.6.1.4.1.16030.1.10.5（附註6）
主體別名 （Subject alternative name）	rfc822	[證書持有人電子郵箱地址]（附註1）
發出人別名（Issuer alternative name）		未使用
基本限制 （Basic constraints）	主體類型 （Subject type）	未使用
	路徑長度限制 （Path length constraint）	未使用
延伸密碼匙使用方法 （Extended key usage）		S/MIME

欄位名稱		欄位內容
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）

附註:

1. 登記人機構提供之中央管理通訊系統功能單位電子郵箱地址。
2. 登記人參考編號：10 位數字。
3. 由中繼證書簽發的證書符合本準則、核證機關／瀏覽器論壇 S/MIME 基線要求。
4. 本欄已包括本核證作業準則的物件識別碼 (Object Identifier, OID)。請參閱本準則第 1.2 條。
5. 證書策略物件識別碼由核證機關／瀏覽器論壇分配給符合機構驗證嚴格證書政策的電子證書。
6. 香港郵政分配物件識別碼顯示，其持有人是政府電子證書（功能單位）之登記人。
7. 證書撤銷清單分發點 URL 為 http://crl1.eCert.gov.hk/crl/eCertCA2-26CRL2.crl，此為中繼證書"Hongkong Post e-Cert CA 2 - 26"所發出的「整體證書撤銷清單」。

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 - 26"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布安排和其格式。

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：

a) **「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 - 26"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"Hongkong Post e-Cert CA 2 - 26"所發出的證書：
http://crl1.eCert.gov.hk/crl/eCertCA2-26CRL1.crl 或
ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post e-Cert CA 2 - 26 CRL1, o=Hongkong Post, 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 point)欄位內註明的位址(URL)獲取相關的證書撤銷清單。

在正常情況下，香港郵政會於更新時間後，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布的時序。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 公布補充證書撤銷清單。

香港郵政會更新及公布授權撤銷清單，而清單內載有已撤銷的中繼證書的資料。香港郵政會每年在其下次更新日期前或在有需要時更新及公布。最新發出的授權撤銷清單可於下述位置下載：

i. 根源證書"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 - 26"根據本準則發出的整體證書撤銷清單格式:-

標準欄位 (Standard Fields)	子欄位 (Sub-fields)	整體證書撤銷清單欄位內容	備註
版本 (Version)		v2	此欄顯示證書撤銷清單格式的版本為 X.509 第二版
簽署算式識別 (Signature algorithm ID)		sha256RSA	此欄顯示用以簽署證書撤銷清單的算法的識別碼
發出人 (Issuer name)		cn=Hongkong Post e-Cert CA 2 - 26, 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)

標準欄位 (Standard Fields)	子欄位 (Sub-fields)	整體證書撤銷清單欄位內容	備註
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)	KeyID	[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
發出人 (Issuer name)		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）			

標準欄位 (Standard fields)	子欄位 (Sub-fields)	授權撤銷清單欄位內容	備註
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. 以下為可於撤銷證書欄位下列出的理由識別碼：

   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，包括交叉證書，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，所有標準延伸欄位均為“非關鍵” (Non-Critical) 延伸欄位。

附錄 D - 香港郵政政府電子證書 – 服務摘要

要點(附註 1)	政府電子證書
登記人機構	香港特別行政區政府決策局／部門／辦公室
登記人	中央管理通訊系統 用戶／中央管理通訊系統 功能單位
依據限額	HK$200,000
認可證書	是
配對密碼匙長度	2048 位元 RSA
核證登記機關	中央管理通訊系統內代表各決策局／部門／辦公室的業務管理人員
產生配對密碼匙	由中央管理通訊系統代製產生
核對身分	如第 3.2 條所述
證書用途	• 加密／解密，及數碼簽署以確認已收訖送出之信息。 • 簽署文件並在中央管理通訊系統內進行認證（不用作 ETO 所述的數碼簽署）（僅限政府電子證書（個人）） • **附錄 H** 列出對應其政府電子證書的指定應用
證書內包含登記人的資料	• 登記人機構名稱 • 中央管理通訊系統用戶英文姓名及其電郵地址（僅限政府電子證書（個人）） • 功能單位用戶英文姓名及其電郵地址（僅限政府電子證書（功能單位）） • 由香港郵政核證機關系統產生的登記人參考編號
登記費用及證書有效期	一年。見**附錄 H**

附註

1. 登記人機構必須先與香港郵政作出安排，香港郵政才可以為登記人機構發出政府電子證書。

附錄 E - 香港郵政政府電子證書登記人機構／核證登記機關名單及中央管理通訊系統(若有的話)

(I) 作為香港郵政登記人機構／核證登記機關的決策局／部門／辦公室名單

作為香港郵政登記人機構／核證登記機關的決策局／部門／辦公室	證書類別	服務提供
漁農自然護理署 建築署 審計署 醫療輔助隊 屋宇署 政府統計處 行政長官辦公室 特首政策組 政務司司長辦公室 - 政府檔案處 政務司司長辦公室及財政司司長辦公室 民眾安全服務處 民航處 土木工程拓展署 公務員事務局 商務及經濟發展局 公司註冊處 政制及內地事務局	政府電子證書（個人）及政府電子證書（功能單位）	為中央管理通訊系統提供以下有關申請政府電子證書之服務： - 根據第3.2條及第4.1條所述提供證書申請服務。 - 根據第4.6條所述提供證書續期請求服務。 - 根據第4.9.1條；第4.9.3條及第4.9.5條所述提供證書撤銷請求服務。 - 根據第5.1.6條所述的決策局／部門／辦公室的文件保存。

作為香港郵政登記人機構／核證登記機關的決策局／部門／辦公室	證書類別	服務提供
懲教署 文創產業發展處 文化體育及旅遊局 香港海關 衞生署 律政司 發展局規劃地政科 發展局工務科 渠務署 教育局 機電工程署 環境及生態局 環境保護署 財經事務及庫務局財經事務科 財經事務及庫務局庫務科 消防處 食物環境衞生署 政府飛行服務隊 政府化驗所 政府物流服務署 政府產業署		

作為香港郵政登記人機構／核證登記機關的決策局／部門／辦公室	證書類別	服務提供
醫務衞生局 路政署 民政事務總署 民政及青年事務局 香港金融管理局 香港天文台 香港警務處 房屋局 房屋署 入境事務處 廉政公署 獨立監察警方處理投訴委員會 政府新聞處 稅務局 創新科技及工業局 創新科技及工業局 - 數字政策辦公室 創新科技及工業局 - 創新科技署 知識產權署 投資推廣署 薪諮會聯合秘書處 司法機構		

作為香港郵政登記人機構／核證登記機關的決策局／部門／辦公室	證書類別	服務提供
勞工及福利局 勞工處 土地註冊處 地政總署 法律援助署 康樂及文化事務署 海事處 通訊事務管理局辦公室 申訴專員公署 破產管理署 規劃署 郵政署 公務員敍用委員會 香港電台 差餉物業估價署 選舉事務處 截取通訊及監察事務專員秘書處 保安局 社會福利署 香港經濟貿易辦事處 工業貿易署		

作為香港郵政登記人機構／核證登記機關的決策局／部門／辦公室	證書類別	服務提供
運輸及物流局 運輸署 庫務署 大學教育資助委員會秘書處 水務署 在職家庭及學生資助事務處(學生資助處) 在職家庭及學生資助事務處(在職家庭津貼辦事處)		

(II) 中央管理通訊系統 (CMMP)

中央管理通訊系統（CMMP）行政及支援	證書類別	提供的服務	備註
數字政策辦公室	香港郵政政府電子證書 (個人)及政府電子證書(功能單位)	設置和維護中央管理通訊系統供決策局／部門／辦公室使用： -提供決策局／部門／辦公室的用戶角色，讓決策局／部門／辦公室以此執行有關政府電子證書的申請； -為證書申請，續期和撤銷提供審批工作流程； -為政府電子證書登記人的私人密碼匙及其使用提供安全保管； -當決策局／部門／辦公室要求時，向其提供政府電子證書登記人的私人密碼匙； 為決策局／部門／辦公室的政府電子證書申請人的提供以下程序： - 為中央管理通訊系統中用戶角色作出定義，使決策局／部門／辦公室能指定人員作為核證登記機關以執行如第 3.2 條所述核證申請人身份。 - 如第 3.2.1, 4.3 及 4.6 所述產生密碼匙。 -承擔第 9.6.5.2 條所述的義務責任。	為達到職責分離的要求，中央管理通訊系統不容許用戶作為“業務管理人員”時批准自己提出的要求，即中央管理通訊系統用戶不能就某一要求同時擔任“業務管理人員”和“提出要求者”的角色。

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

由本核證作業準則生效日期起，就此核證作業準則而言，香港郵政政府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。
主體專有名稱 （Subject DN） C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 2 SHA-1 Thumbprint DE010808E41EC41930D44095F8FE596B582C8CA2			
2	Hongkong Post e-Cert CA 2 - 26	2026 年 5 月 7 日 至 2040 年 9 月 5 日	此中繼證書由 2026 年 10 月 1 日起開始發出政府電子證書。
主體專有名稱 （Subject DN） C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert CA 2 - 26 SHA-1 Thumbprint EA9AECB58CB9023AE090235EA2FFFA8ED8420A88			

附錄 H - 香港郵政政府電子證書相對應之指定應用

政府電子證書類別	證書有效期	指定應用	登記費	備註
政府電子證書（個人）	1 年	由中央管理通訊系統支援的數字政策辦公室之應用	新申請或續期：每份證書每年港幣 20 元。 承辦商就政府電子證書（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。	第 1.3.4.1.1 條所述政府電子證書（個人）的用途
政府電子證書（功能單位）	1 年	由中央管理通訊系統支援的數字政策辦公室之應用	新申請或續期：每份證書每年港幣 20 元。	第 1.3.4.1.2 條所述政府電子證書（功能單位）的用途