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
智能身份證電子證書（個人）
核證作業準則

日期：二零零三年七月二十二日

目錄

前言

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

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

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

根據條例所載規定，就條例及公匙基建而言，香港郵政署長爲認可核證機關。根據條例，香港郵政署長可透過香港郵政署職員履行核證機關之職能並提供服務。香港郵政署長已決定履行其職能，而就此文件而言，其身分爲**香港郵政**。

根據條例，香港郵政爲認可核證機關，負責使用穩當系統發出、撤回及利用公開儲存庫公佈已認可及已接受之數碼證書作爲在網上進行穩妥的身分辨識。根據本核證準則發出的電子證書（個人），在本核證準則內稱爲“證書”或“電子證書”。

香港郵政發出可載入智能身份證內的個人電子證書。另外，在香港郵政及登記人的同意下，個人電子證書亦可載入其他存儲介質，如軟磁碟、智能卡等。

本核證作業準則之結構如下：

第 1 條載有概述及聯絡資料
第 2 條列載各方責任及義務
第 3 條列載申請及身分確認程序
第 4 條載述運作要求
第 5 條介紹保安監控措施
第 6 條列載如何產生及監管公開/私人配對密碼匙
第 7 條簡介技術要求
第 8 條敘述如何管理本核證作業準則

附錄 A - 詞彙表
附錄 B – 香港郵政電子證書（個人）格式
附錄 C – 香港郵政電子證書撤銷清單格式
附錄 D – 香港郵政電子證書（個人）特點摘要

1． 引言

1.1 概述

本核證作業準則（“準則”）由香港郵政公佈，使公眾有所瞭解，並規定香港郵政在發出、撤回及公佈可加入智能身份證內的電子證書時採用之做法及標準。

香港郵政已獲 Internet Assigned Numbers Authority (IANA) 分配私人企業號碼 (Private Enterprise Number) 16030 號。「1.3.6.1.4.1.16030.1.1.2」爲本準則的物件識別碼 (Object Identifier, OID)（見附錄 B 內關於核證政策(Certificate Policies)的說明）。

本準則列載參與香港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證書人士之倚據並用來核實數碼簽署。接受由香港郵政發出之證書之各倚據證書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，可用來認證各倚據證書人士之特定公匙基建應用程序上之參與者之身分。

根據條例，香港郵政爲認可核證機關。而根據本核證作業準則而發出的電子證書（個人），香港郵政已指明爲認可證書。對登記人及倚據證書人士而言，根據該條例香港郵政在法律上有義務使用穩當系統，發出、撤回及在可供公眾使用之儲存庫公佈獲接受之認可證書。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，包括陳述此等證書爲按照本準則發出者（下文詳述其定義）。

附錄 D 載有香港郵政電子證書（個人）特點摘要

1.2 社區及適用性

1.2.1 核證機關

根據本準則，香港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（見第 2.1.1 條）。

1.2.1.1 香港郵政所作之陳述

根據本準則而發出之證書，香港郵政向根據本準則第 2.1.3 條及其他有關章條之倚據證書人士表明，香港郵政已根據本準則發出證書。透過公佈本準則所述之證書，香港郵政即向根據本準則第 2.1.3 條及其他有關章條之倚據證書人士表明，香港郵政已根據本準則發出證書予其中已辨識之登記人。

1.2.1.2 生效

經香港郵政簽署之證書一經發出並由登記人接受，香港郵政將迅速於儲存庫公佈已發出之證書。（見第 2.5 條）

1.2.1.3 香港郵政進行分包合約之權利

經登記人在登記人協議中同意後，只要分包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，批予分包商執行。無論有關職務是否批出由分包商執行，香港郵政仍會負責履行本準則及登記人協議。

1.2.2 最終實體

根據本核證作業準則，存在兩類最終實體，包括登記人及倚據證書人士。登記人乃已獲發出電子證書之個人。倚據證書人士乃於交易中依據電子證書之實體。於交易中依據其他登記人之電子證書之申請人及登記人乃爲有關此證書之倚據證書人士。**請倚據證書人士留意，香港郵政電子證書系統並無年齡限制，未成年人仕可申請並領取電子證書。**

1.2.2.1 登記人之保證及陳述

各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（尤其是倚據證書人士）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) 除證書登記人外，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（個人）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) 證書所載之所有資料及由登記人作出之陳述均屬真實。
d) 證書將只會用於符合準則之認可及合法用途。
e) 在證書申請過程中所提供之所有資料，均並無侵犯或違反任何第三方之商標、服務標記、品牌、公司名稱或任何知識產權。

1.2.3 登記人之類別

根據本準則香港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。根據本準則和登記人協議，電子證書（個人）會發出予持有香港身份證人仕。此等證書可用來從事商業經營。電子證書（個人）可發出予持有香港身份證之十八歲以下人士（另見第 3.1.1.2 段）。

1.2.4 證書之期限

根據本核證作業準則發出予新申請人之證書有效期爲三年。根據本核證作業準則之證書續期程序而發出之證書有效期可超過三年，但不會超過三年另一個月 (見第 3.3 條證書續期)。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。

1.2.5 在香港郵政處所進行申請

對於所有首次申請及證書撤銷或到期後之申請，申請人須依據第 3.1 及 4.1 段指明的程序遞交申請。

1.3 聯絡資料

登記人可經由以下途徑作出查詢、建議或投訴：
郵寄地址：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@hongkongpost.gov.hk

1.4 處理投訴程序

香港郵政會盡快處理所有以書面及口頭作出的投訴，並在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。

2． 一般規定

2.1 義務

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。無論登記人是否亦爲有關其他登記人證書之倚據證書人士，均須如此。關於非登記人倚據證書人士，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準則發出、收回及公佈證書時對倚據證書人士造成若干類型之損失及損害，並就下文及所發出之證書所載之責任限定幣值。

2.1.1 核證機關之義務

根據條例，香港郵政爲認可核證機關，負責使用穩當系統發出、撤回及利用公開儲存庫公佈已獲登記人接受之認可證書。根據本準則，香港郵政有下述義務：

a) 依時發出及公佈證書（見第 2.5 條），
b) 通知申請人有關已批準或被拒絕的申請（見第 4.1 條），
c) 撤銷證書及依時公佈證書撤銷清單（見第 4.4 條），
d) 通知登記人有關已撤銷的證書（見第 4.4.1., 4.4.2. 及 4.4.3 條），

2.1.2 登記人之義務

登記人負責：

a) 同意香港郵政代表登記人，在香港郵政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。
b) 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；履行該協議規定其應承擔之義務及確保在申請證書時所作的陳述準確無誤。
c) 準確地按照本準則所載關於完成證書之程序。
d) 承認承諾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、洩露或未經授權使用之義務。
e) 發現其證書的私人密碼匙之任何丟失或外洩時，立即呈報丟失或外洩（外洩乃屬違反保安，使資料遭受未經授權之進入，從而導致未經授權即對資料進行披露、更改或使用）。
f) 不時將登記人提供之證書資料之任何變動立即通知予香港郵政。
g) 將可能致使香港郵政根據下文第 4 條所載之理由行使權利，撤銷由該登記人負責之證書之任何事項立即通知予香港郵政。
h) 同意其透過獲發出或接受證書向香港郵政保證（承諾）並向所有倚據證書人士表明，在證書之有效期間，以上第 1.2.2.1 條載明之事實乃屬真實並將一直保持真實。
i) 在登記人明知香港郵政根據準則條款可能據以暫時吊銷或撤銷證書之任何事項之情況下，或登記人已作出撤銷申請或經香港郵政知會，香港郵政擬根據本準則之條款暫時吊銷或撤銷證

書後，均不得在交易中使用證書。

j) 在明知香港郵政可能據以暫時吊銷或撤銷證書之任何事項之情況下，或登記人作出撤銷申請或經香港郵政知會擬暫時吊銷或撤銷證書時，須立即通知從事當時仍有待完成之任何交易之倚據證書人士，用於該交易之證書須予暫時吊銷或撤銷(由香港郵政或經登記人申請)，並明確說明，因情形乃屬如此，故倚據證書人士不得就交易而倚據證書。

k) 如登記人的智能身份證已遺失、損毀、污損或損壞，或已向入境事務處或其他執法機關退回其智能身份證，或其智能身份證已被入境事務處或其他執法機關根據香港特別行政區法例終止有效或扣押，登記人同意放棄使用任何載於該智能身份證內的私人密碼匙。登記人亦同意香港郵政，及香港特別行政區政府，在此等事宜上對申請人或登記人並不負有任何責任。申請人/登記人可根據第 4.4.2 段說明的程序，要求香港郵政撤銷載於智能身份證內的電子證書

2.1.2.1 登記人之責任

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

2.1.3 倚據證書人士之義務

倚據香港郵政電子證書之倚據證書人士負責：

a) 倚據證書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，確定使用證書乃適合本準則規定之用途，尤其考慮到香港郵政向倚據證書人士承擔本準則及證書所載之謹慎職責及金錢責任乃屬有限。

c) 於倚據證書前查核證書撤銷清單上證書狀態。

d) 執行所有適當證書路徑認可程序。

2.2 其他規定

香港郵政對登記人及倚據證書人士之義務

2.2.1 合理技術及謹慎

香港郵政謹此與各登記人協議，根據本準則香港郵政向各登記人及倚據證書人士履行及行使作爲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證書人士承擔任何絕對義務。**香港郵政不保證其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，儘管香港郵政於執行本合約及其根據準則應有之權利及義務時採取合理程度之技術及謹慎，若登記人作爲準則定義下之登記人或倚據證書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，各登記人同意香港郵政無需承擔任何責任、損失或損害。

即如香港郵政已採取合理程度之技術及謹慎之前提下，若登記人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僞造之數碼簽署而蒙受損失或損害，香港郵政概不負責。

亦即如在香港郵政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，若登記人因香港郵政不能控制之情況遭受不良影響，香港郵政概不負責。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爲。

2.2.2 非商品供應

特此澄清，登記人協議並非任何性質商品之供應合約。任何及所有據此發出之證書持續爲香港郵政之財產及爲其擁有且受其控制，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爲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證書人士接達之公開儲存庫內提供之證書，並非作爲對倚據證書人士供應任何商品；亦不會作爲對倚據證書人士關於證書爲某一特定目的之可商售性或適用性的保證；亦不會作爲向倚據證書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免費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，香港郵政須承擔下文第 2.2.3 至 2.2.4 條所述責任。另外，電子證書客戶套件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，而須由電子證書客戶套件內另行載述之條文決定。

2.2.3 法律責任限制

2.2.3.1 限制之合理性

各登記人及倚據證書人士承認並同意公開密碼匙基礎建設及香港郵政於系統範圍內作爲核證機關乃嶄新業務。根據此系統，倘若香港郵政負法律責任，且對根據公開密碼匙基礎建設因或與本登記人協議相關或與香港郵政發出證書相關香港郵政所蒙受損害沒有加以限制，香港郵政從登記人處接受金額將比該法律責任小得多。因此，各登記人或倚據證書人士必須同意，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。

2.2.3.2 可追討損失種類之限制

在香港郵政違反：

a) 本登記人協議；或

b) 任何謹慎職責－尤其當登記人或倚據證書人士、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，爲登記人或倚據證書人士，而採取合理技巧及謹慎及/或職責

的情況下，而登記人或倚據證書人士（無論作爲根據準則或以其他任何方式定義之登記人或倚據證書人士）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。**

2.2.3.3 限額 -- 20 萬港元（電子證書（個人））

除下文所述例外情況外，在香港郵政違反：

a) **本登記人協議或本核證作業準則的條款；或**

b) **任何謹慎職責－尤其當登記人或倚據證書人士、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－應根據登記人協議、本準則、或法例，爲登記人或倚據證書人士，採取合理技巧或謹慎及/或職責**

之情況下，而登記人或倚據證書人士蒙受損失及損害（無論作爲根據準則或以其他任何方式定義之登記人或倚據證書人士），對於任何登記人、或任何倚據證書人士（無論作爲根據準則或以其他任何方式定義之登記人或倚據證書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不得超過每份電子證書（個人）20 萬港元、或每份發出予未滿 18 歲人仕的電子證書（個人）0（零）港元。

2.2.3.4 提出索償之時限

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

2.2.3.5 香港郵政署人員

無論香港郵政署或其任何職員或僱員或其他代理人均非登記人協議之簽約人，登記人及倚據證書人士必須向香港郵政承認，就登記人及倚據證書人士所知，香港郵政署及其所有職員、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爲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、或倚據證書人士擔負任何個人責任或謹慎職責；每一位登記人及倚據證書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爲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個人免受此等法律行動。

2.2.3.6 蓄意之不當行爲或個人傷亡之責任

任何因欺詐或蓄意之不當行爲或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。

2.2.3.7 證書通知、限制及倚據限額

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，根據電子交易條例作爲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準則（可瀏覽 http://www.hongkongpost.gov.hk）。香港特別行政區法律適用於本證書，倚據證書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。

倘閣下爲倚據證書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，其職員、僱員及代理人）發出本證書，但無須對倚據證書人士承擔任何責任或謹慎職責（準則中列明者除外）。

倚據證書人士倚據本證書前負責：

a. 只有當倚據證書人士於倚據時所知之所有情況證明倚據行爲乃屬合理及本著真誠時，方可倚據本證書；
b. 倚據本證書前，確定證書之使用就準則規定之用途而言乃屬適當；
c. 倚據本證書前，根據證書撤銷清單檢查本證書之狀態；及
d. 履行所有適當證書路徑認可程序。

若儘管香港郵政署長及香港郵政署、其職員、僱員或代理人已採取合理技術及謹慎，本證書仍在任何方面不準確或誤導，則香港郵政署長、香港郵政署、其職員、僱員或代理人對倚據證書人士之任何損失或損害概不承擔任何責任，在該等情況下根據條例適用於本證書之倚據限額爲 0 港元。

若本證書在任何方面不準確或誤導，而該等不準確或誤導乃因香港郵政署長、香港郵政署、其職員、僱員或代理人之疏忽所導致，則香港郵政署長將就因合理倚據本證書中之該等不準確或誤導事項而造成之經證實損失向每名倚據證書人士支付最多 20 萬港元（如該證書爲電子證書（個人））、或支付最多 0（零）港元（如該證書爲發出予未滿 18 歲人仕

的電子證書（個人），惟該等損失不屬於及不包括（1）任何直接或間接利潤或收入損失、信譽或商譽損失或傷害、任何商機或契機、失去工程或失去或無法使用任何數據、設備或軟件或（2）任何間接、相應而生或附帶引起之損失或損害，而且即使在後者情況下，香港郵政已被提前通知此類損失或損害之可能性。在該等情況下根據條例適用於本證書之倚據限額爲 20 萬港元（如該證書爲電子證書（個人））、或 0（零）港元（如該證書爲發出予未滿 18 歲人仕的電子證書（個人）），而在所有情形下就第（1）及（2）類損失而言倚據限額則爲 0 港元。

在任何情況下，香港郵政署、其職員、僱員或代理人概不對倚據證書人士就本證書承擔任何謹慎職責。

索賠時限

任何倚據證書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、撤回或公佈任何證書相關，則應在倚據證書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、其職員、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證書人士所應承擔之法律責任作出任何限制。

本文所載之法律責任限制不適用於個人傷害或死亡之（不大可能發生之）情形。”

2.2.4 香港郵政對有缺陷之客戶套件或唯讀光碟（或替代存儲介質）或軟磁碟或其他存儲介質及已接受但有缺陷之電子證書所承擔之責任

2.2.4.1 儘管上文已列明承擔責任之限制，假如因根據本準則而提供給登記人的電子證書客戶套件或唯讀光碟（或替代存儲介質）或軟磁碟或其他存儲介質（“套件”）有缺陷以致提供之有關證書未能或無法完成或接受妥當，而接收“套件”之登記人即時在送出“套件”三個月內發出通知讓香港郵政安排更換（如願意接受），若登記人無意再擁有證書，而香港郵政同意缺陷確實存在，有關費用即可退還。若登記人在“套件”送出三個月過後方通知香港郵政，則費用不會自動退還，而需由香港郵政酌情退回。特此澄清，智能身份證乃由入境事務處發出，而非由香港郵政根據本準則而提供。

2.2.4.2 儘管上文已列明香港郵政承擔責任之限制，若登記人接受證書後發現，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（如願意接受）重新發出。或倘此通知已於接

受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。倘登記人於接受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，而需由香港郵政酌情退回。

2.2.5 登記人的轉讓

登記人不可轉讓登記人協議或證書賦予之權利。擬轉讓之行爲均屬無效。

2.2.6 陳述權限

除非獲得香港郵政授權，香港郵政署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。

2.2.7 更改

香港郵政有權更改本準則，而無須發出預先通知(見第 8 條)。登記人協議不得作出更改、修改或變更，除非符合本準則中之更改或變更規定，或獲得香港郵政署長之明確書面同意。

2.2.8 保留所有權

根據本準則發出之證書上所有資料之實質權利、版權及知識產權現屬香港郵政所有，日後亦然。

2.2.9 條款衝突

倘本準則與其他規則、指引或合約有衝突，登記人、倚據證書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。

2.2.10 受信關係

香港郵政並非登記人或倚據證書人士之代理人、受信人、受託人或其他代表。登記人及倚據證書人士無權以合約或其他方式約束香港郵政承擔登記人或倚據證書人士之代理人、受信人、受託人或其他代表之責任。

2.2.11 相互核證

香港郵政在所有情形下均保留與另一家核證機關或郵政核證機關定義及確定適當理由進行相互核證之權利。

2.2.12 財務責任

保單已經備妥，有關證書之潛在或實質責任以及對倚據限額之索償均獲承保。

2.3 解釋及執行（管轄法律）

2.3.1 管轄法律

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

2.3.2 可中止性、尚存、合併及通知

若本準則之任何條款被宣佈或認爲非法、不可執行或無效，則應刪除其中任何冒犯性詞語，直至該等條款成爲合法及可執行爲止，同時應保留該等條款之本意。本準則之任何條款之不可執行性將不損害任何其他條款之可執行性。

2.3.3 爭議解決程序

香港郵政關於本準則範圍內之事宜之決定爲最終決定。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@hongkongpost.gov.hk

2.3.4 詮釋

本準則中英文本措詞詮釋若有歧異，則以英文本爲準。

2.4 登記費用

每份電子證書（個人）（包括首次及續期申請）年費爲 50 港元（登記費用）。 香港郵政會豁免首年的證書費用，使每位智能身份證持有人可享有首年免費使用首份加入智能身份證內的電子證書。除非獲得香港郵政豁免（就首年而言），否則登記人需在每一有效登記時段開始前，繳付登記費用。香港郵政保留經常檢討及決定登記費用的絕對權利，及會利用其網頁（http://www.hongkongpost.gov.hk）通知登記人及公眾。

2.5 公佈資料及儲存庫

香港郵政維持一儲存庫，內有根據本核證作業準則簽發並已經由登記人接受的證書清單、最新證書撤銷清單、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。除每週最多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。香港郵政在收到登記人確認接受電子證書後，會儘快在儲存庫公佈該證書。香港郵政儲存庫可透過下述 URL 接達：

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

2.5.1 證書儲存庫控制

儲存庫所在位置可供在線瀏覽，並可防止擅進。

2.5.2 證書儲存庫進入要求

經授權之香港郵政僱員方可進入儲存庫更新及修改內容。

2.5.3 證書儲存庫更新週期

每份證書一經登記人接受或例如撤銷證書或其他核證機關披露記錄情況一旦發生，儲存庫均會即時更新。

2.6 遵守規定之評估

須根據香港法例第 553 章電子交易條例以及認可核證機關守則之規定，至少每 12 個月進行一次遵守規定之評估，查清香港郵政發出、撤回及公佈證書之系統是否妥善遵守本準則。

2.7 機密性

香港郵政會確保本身及履行與香港郵政發出、撤回及公佈證書之有關任務之任何香港郵政分包商均會依循此條限制事項。作爲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；香港郵政需根據本準則履行其責任之情況除外。除非經法庭發出之傳召或命令要求，或香港法例另有規定，否則未經登記人事先同意，不得將該等資料對外發布。除非法庭發出傳票或命令，或香港法例另有規定，香港郵政尤其不得發表登記人清單或其資料，惟無法追溯個別人登記人之綜合資料除外。

3． 鑑別及認證

3.1 首次申請

除非申請人爲電子 證書（個人）之持有人，否則各證書申請人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，並出示第 3.1.8 條所述身分證明。如申請人爲電子 證書（個人）之持有人，則無須親身呈遞， 但須提交申請人的數碼簽署（須由申請人的電子證書（個人）證明）作爲身份證明。

所有證書申請人須向香港郵政呈交一份填妥之申請表及登記人協議。申請獲承認後，香港郵政即準備證書並向申請人發出通知，說明如何發出及接受證書。

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可識別電子證書（個人）登記人之身分，該名稱由以下資料組成：

a) 登記人香港身份證上顯示之登記人姓名，及

b) 儲存於證書內的登記人香港身份證號碼的雜湊數值 (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)

此等登記人識別方法同上。登記人如在遞交電子證書申請表時未滿 18 歲，其獲發出的證書會展示 ”e-Cert (Personal/Minor)”（意即「電子證書（個人/未成年人仕）」）字樣（見附錄 B），以顯示登記人在遞交電子證書申請表時未滿 18 歲。

3.1.2 名稱需有意義

所採用名稱之語義必須爲一般人所能理解，方便辨識登記人身分。

3.1.3 詮釋各個名稱規則

香港郵政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。有關香港郵政電子證書主體名稱之詮釋應參照附錄 B。

3.1.4 名稱獨特性

對登記人而言，主體名稱所有部分(包括登記人參考編號)合而爲一整體時應無歧義而具獨特性。然而，此準則並不要求名稱某一特別部分或成分本身具獨特性或無歧義。

3.1.5 名稱申索爭議決議程序

香港郵政對有關名稱爭議之事宜的決定爲酌情性及最終決定。

3.1.6 侵犯及違反商標註冊

申請人及登記人向香港郵政保證（承諾）並向倚據證書人士申述，申請證書過程提供之資料概無以任何方式侵犯或違反第三者之商標權、服務商標、商用名稱、公司名稱或知識產權。

3.1.7 證明擁有私人密碼匙之方法

香港郵政爲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以本核證作業準則第 4.1.2、4.2.3、4.3.1.2、4.3.1.3 及 4.3.2.2 條中指明的安全方式交付予登記人。

3.1.8 個人身分認證

各申請人身分之確認將透過如下運作完成：

a) 各證書申請人可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，出示填妥並已簽署之申請表及登記人協議以及申請人香港身份證。該前述處所人員將覆核並認證所有申請文件，隨後將申請遞轉交香港郵政核證機關處理。
b) 各證書申請人可出示由其電子證書（個人）證明的數碼簽署。

3.2 續付登記費

3.2.1 香港郵政會於證書的免費使用期屆滿前前一個月內以電子郵件或信件向登記人發出續期通知。所有發出並載於智能身份證內電子證書的有效期爲 3 年，而智能身份證持有人可免費使用該證書 1 年。續付登記費可因應登記人的要求及香港郵政的酌情權，在證書的免費使用期屆滿前辦理。香港郵政不會爲過期、已暫時吊銷或已撤銷的證書辦理續付登記費。

3.2.2 在證書的 3 年有效期內，智能身份證持有人不須前往香港郵政服務櫃位在智能身份證內加入另一電子證書。如智能身份證持有人未能在證書的免費使用期屆滿前續付登記費，其證書可被撤銷。該證書可繼續存於智能身份證內。智能身份證持有人亦可前往指定郵政局要求移除智能身份證內的電子證書。

3.2.3 爲電子證書（個人）續付登記費不須進行身份認證（遞交新證書申請時，須對申請人進行身份認證）。申請續付登記費，登記人可以電子方式遞交申請、或填妥及簽署一份續付登記費申請表予香港郵政。續付登記費的資料，可於郵政局及香港郵政網頁取得。續付登記費以後，登記人的電子證書及私人密碼匙會繼續有效，而不須爲登記人製作新的配對密碼匙。續付登記費以後，只要登記人協議原有之條款及條件與續付登記費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該證書。如兩者有所抵觸，則以續付登記費當日之核證作業準則內的條款爲準。申請人應細閱當日有效的核證作業準則，方可遞交續付登記費申請表。

3.3 證書續期

3.3.1 香港郵政會於證書的有效期屆滿前一個月內，以電子郵件或信件向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。香港郵政不會爲過期、已暫時吊銷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可由證書產生日期起有效，而有效期會於原有證書（即須續期的證書）到期日的三年後屆滿。由此，新證書的有效期可超過三年，但不會超過三年另一個月。

3.3.2 每一電子證書(個人)可續期而無須如首次申請時般進行認證登記人身分的程序申請續期時，登記人可透過電子方式或填寫並簽署證書續期申請表向香港郵政遞交申請。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.hongkongpost.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爲準。申請人應細閱續期當日有效的核證作業準則，方可遞交續期申請表。

4． 運作要求

4.1 證書申請

4..1.1 處理申請

4.1.1.1　未獲發給智能身份證的市民可經以下途徑申請將電子證書載入智能身份證內（見第 4.2 段）：

a) 在前往入境事務處的智能身份證中心辦理更換身份證手續前，親自到香港郵政服務櫃位、以郵遞、傳真或經互聯網預先遞交電子證書申請表；或

b) 在入境事務處的智能身份證中心辦理更換身份證手續時，於設於智能身份證中心內的香港郵政服務櫃位遞交電子證書申請表。

4.1.1.2　已獲發給智能身份證但未申請在智能身份證載入電子證書的市民可於指定香港郵政服務櫃位申請將電子證書載入智能身份證內（見第 4.3.1 段）。

4.1.1.3　市民可於指定香港郵政服務櫃位申請電子證書，並將電子證書存儲在軟磁碟或替代存儲介質上（智能身份證以外的存儲介質）（見第 4.3.2 段）。

4.1.2 電子證書及私人密碼匙備份

4.1.2.1　如智能身份證已遺失或損壞，該智能身份證內的電子證書（包括其私人密碼匙）將不能復原。就此，申請人可選擇付費獲取其在智能身份證內的電子證書及其私人密碼匙的備份。該備份會存儲於軟磁碟或替代存儲介質上。申請人可於遞交電子證書申請表時，選取備份電子證書及私人密碼匙的選項。

4.1.2.2　如申請人已選擇電子證書備份，以申請人的個人密碼保護的私人密碼匙及證書將隨後被存儲在軟磁碟或替代存儲介質上。軟磁碟或替代存儲介質會密封於一可防止改動的封套或其他容器內；並以申請表中指明的方式交付予登記人。

4.1.2.3　申請人同意，他們一旦接獲磁片或替代存儲介質，即須完全爲私人密碼匙的安全保管負責，並且同意，他們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。

4.1.2.4　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。

4.1.3 核對身份

4.1.3.1　申請人須於香港郵政服務櫃位，向香港郵政職員出示其香港身份證，以核對身份。完成核對身份手續後，申請人會收到一個電子證書「個人密碼信封」。

4.1.3.2　每份載入智能身份證內的電子證書及私人密碼匙均由個別的「電子證書個人密碼」保護。「電子證書個人密碼」會另外以密碼信封形式分發給電子證書申請人。在隨後使用電子證書及私人密碼匙時，均需要該「電子證書個人密碼」以防範電子證書及私人密碼匙在未經準許情況下被接達。

4.1.3.3　香港郵政會以電子郵件或郵寄信件通知申請人申請已獲批核。若香港郵政未能根據本準則列明的要求成功核實有關申請，香港郵政會拒絕有關申請並通知申請人。

4.2 發出電子證書及經入境事務處將電子證書載入智能身份證內

4.2.1　在第 4.1.1.1 段指明的地點遞交的申請，香港郵政會透過在本 4.2 段列明的程序發出可載入申請人智能身份證內的電子證書；以便申請人可於入境事務處領取已載有電子證書的智能身份證。

4.2.2 確定資料

4.2.2.1　入境事務處與香港郵政雙方的電腦系統會每天進行下述的確定資料的程序：

a) 已申請電子證書市民的資料會穩妥地存儲於由香港郵政開發及管理的數據庫內；

b) 經預先設定，香港郵政的系統會每天整理一份「申請人名單」；列出屬於當日更換身份證組別（於憲報刊登）的電子證書申請人的身份證號碼及英文姓名；

c) 香港郵政的系統會每天將「申請人名單」，經由設有終端加密的穩妥通訊線路，傳送到入境事務處的系統，以進行確定資料的程序；

d) 入境事務處的系統會根據「申請人名單」內各申請人的身份證號碼，確定各申請人是否已登記更換身份證。入境事務處的系統並會將一份列有申請人狀況（"已確定" 或 "未能確定"）的「確定結果名單」傳回香港郵政的系統。入境事務處不會保留「申請人名單」或「確定結果名單」的副本；及

e) 入境事務處系統與香港郵政系統之間的數據傳送，均經由設有終端加密的穩妥通訊線

路傳輸。

4.2.2.2　上述確定資料的程序不會構成在個人資料（私隱）條例（香港法例第 486 章）內指明的「核對程序[1]」。進行上述確定資料程序的目的，是要確定有關的電子證書申請人已登記更換身份證，以便香港郵政可製作申請人的電子證書，並將電子證書傳送至入境事務處及載入申請人的智能身份證內。上述確定資料的程序並非以引致香港郵政對電子證書申請人（作爲 "資料當事人"）作出「不利行動[2]」爲目的。上述確定資料的程序不會剝奪市民享有一年免費使用載於智能身份證內電子證書的機會。香港郵政會跟進在確定資料程序中 "未能確定" 的申請人資料，使他們可將電子證書及私人密碼匙載入智能身份證內。

4.2.3 製作及將電子證書載入智能身份證內

4.2.3.1　經過確定資料程序後，香港郵政會爲 " 已確定" 的申請人製作電子證書（相關的配對密碼匙）；並將電子證書及私人密碼匙傳送至入境事務處及載入申請人的智能身份證內。香港郵政代表登記人產生配對密碼匙，而香港郵政製作證書。在香港郵政的處所內有一套可靠的系統及環境來進行上述作業，以保證私人密碼匙不受干擾。

4.2.3.2 將電子證書及私人密碼匙載入智能身份證內的流程如下：

a) 香港郵政會將電子證書及私人密碼匙（由「電子證書個人密碼」保護（見第 4.2.2.2 段）及已加密）經由設有終端加密的穩妥通訊線路傳輸至入境事務處。已加密的電子證書及私人密碼匙會存於入境事務處的穩妥系統內以便載入智能身份證內;
b) 入境事務處的系統會將個別已加密的電子證書及私人密碼匙載入配對的智能身份證內; 及
c) 入境事務處的系統會將已加密的電子證書及私人密碼匙從其數據庫中刪除。

4.2.4 接受電子證書

4.2.4.1　香港郵政會爲智能身份證持有人提供合理機會，從入境事務處領取智能身份證後，確認接受其電子證書。申請人同意，他們一旦接獲智能身份證，即須完全爲載於智能身份證內的私人密碼匙的安全保管負責，並且同意，他們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。接受電子證書可經由第 4.2.4.2 段（經由香港郵政網頁）或 4.2.4.3 段（經由香港郵

[1] 根據個人資料（私隱）條例，"核對程序" (matching procedure) 指將爲 1 個或 1 個以上的目的而取自 10 個或 10 個以上的資料當事人的個人資料與爲其他目的而自該等資料當事人收集的個人資料比較的程序(用人手方法的除外)，而—
(a) 所作比較(不論是全部的還是部分的)是爲了產生和核實某些可(即時或於其後任何時間)用作對任何該等資料當事人採取不利行動的資料的；或
(b) 所作比較產生和核實某些資料，而就該等資料而言可合理地相信將該等資料(即時或於其後任何時間)用作對任何該等資料當事人採取不利行動是切實可行的；

[2] 根據個人資料（私隱）條例，"不利行動" (adverse action)，就個人而言，指可對該人的權利、利益、特權、責任或權益(包括合法期望)有不利影響的任何行動。

政服務櫃位）說明的步驟完成。

4.2.4.2 申請人可經互聯網在指定的香港郵政網頁上完成以下步驟確認接受其電子證書：

a) 申請人在網頁輸入其個人資料；
b) 如申請人所輸入資料與香港郵政系統所存有的資料吻合，申請人的電子證書內容會展示，以申請人便核實；
c) 申請人可確認接受電子證書（見第 4.2.4.4 段）；
d) 申請人確認接受電子證書的資料會傳回香港郵政系統。

4.2.4.3 申請人可於指定香港郵政服務櫃位完成以下步驟確認接受其電子證書：

a) 將智能身份證插入安裝於服務櫃位上電腦的智能卡閱讀器內；
b) 展示智能身份證內的電子證書內容，以便智能身份證持有人核實；
c) 智能身份證持有人確認接受電子證書（見第 4.2.4.4 段）；
d) 申請人確認接受電子證書的資料會傳回香港郵政系統。

4.2.4.4 在上述第 4.2.4.2(c)段及第 4.2.4.3(c)段所述程序中，申請人亦可確認不接受其電子證書及要求撤銷其電子證書。申請人可將 ″不接受″ 的電子證書繼續存於智能身份證上、或到指定郵政局將電子證書移除。

4.2.5 公佈電子證書

在登記人確認接受其電子證書後，香港郵政會根據電子交易條例的要求，於香港郵政的儲存庫公佈已獲接受的電子證書（見第 2.5 段）。未獲接受的電子證書紜不會於香港郵政的儲存庫公佈。

4.3 在香港郵政服務櫃位發出電子證書

4.3.1 在香港郵政服務櫃位發出電子證書並載入智能身份證內

4.3.1.1 就獲發給智能身份證後才決定申請電子證書人仕、及” 未能確定資料”人仕（見第 4.2.2 段），此等人仕可於指定香港郵政服務櫃位辦理申請電子證書及將證書載入其智能身份證內。指定香港郵政服務櫃位的位置刊登於香港郵政網址 www.hongkongpost.gov.hk.

4.3.1.2 獲發給智能身份證後才決定申請電子證書人仕，可於指定香港郵政服務櫃位，經以下程序辦理申請電子證書及將證書及私人密碼匙載入其智能身份證內：

a) 申請人根據第 4.1.1.2、4.1.2 及 4.1.3 段所述程序遞交申請表、完成核對身份及領取密碼信封；
b) 香港郵政職員會使用電腦終端機輸入申請人在申請表上提供的資料，以製作電子證書；

c) 已製作電子證書的內容會在顯示屏上展示，以便申請人核實；
d) 申請人可確認接受電子證書（見第 4.2.4 段）；確認接受電子證書的資料會傳回香港郵政系統；
e) 如申請人確認接受電子證書，申請人的智能身份證會放進智能卡閱讀器內。申請人的電子證書及私人密碼匙會經由穩妥的機制從後端的穩妥系統內提出並載入智能身份證內。載入的電子證書已由申請人密碼信封內的電子證書個人密碼保護。如申請人拒絕確認接受電子證書，其智能身份證將不會載入電子證書及私人密碼匙；
f) 當上述程序完成後，該智能身份證會即時交回申請人；
g) 已獲接受的電子證書會在儲存庫內公佈。

4.3.1.3 ”未能確定資料”的申請人，可經以下程序辦理申請電子證書及將證書及私人密碼匙載入其智能身份證內：

a) 申請人向香港郵政職員出示智能身份證，以便香港郵政職員經由櫃位電腦終端機核對其申請狀況；
b) 根據香港郵政系統內的申請人紀錄，如確定申請人已遞交申請表、完成核對身份及領取密碼信封，香港郵政職員會安排經由櫃位電腦終端機製作申請人的電子證書；
c) 已製作電子證書的內容會在顯示屏上展示，以便申請人核實；
d) 申請人可確認接受電子證書（見第 4.2.4 段）；確認接受電子證書的資料會傳回香港郵政系統；
e) 如申請人確認接受電子證書，申請人的智能身份證會放進智能卡閱讀器內。申請人的電子證書及私人密碼匙會經由穩妥的機制從後端的穩妥系統內提出並載入智能身份證內。載入的電子證書及私人密碼匙已由申請人密碼信封內的電子證書個人密碼保護。如申請人拒絕確認接受電子證書，其智能身份證將不會載入電子證書及私人密碼匙。
f) 當上述程序完成後，該智能身份證會即時交回申請人；
g) 已獲接受的電子證書會在儲存庫內公佈。

4.3.2 在香港郵政服務櫃位發出電子證書並載入軟磁碟或替代存儲介質內

4.3.2.1 欲申請存儲在軟磁碟或替代存儲介質（智能身份證除外）上的電子證書的人仕，可於指定香港郵政服務櫃位辦理申請電子證書手續。指定香港郵政服務櫃位的位置刊登於香港郵政網址 www.hongkongpost.gov.hk.

4.3.2.2 市民可於指定香港郵政服務櫃位，經以下程序辦理申請電子證書及領取存儲在軟磁碟或替代存儲介質上的電子證書：

a) 申請人根據以下程序遞交申請表、完成核對身份及領取密碼信封：
   - 申請人於香港郵政服務櫃位，向香港郵政職員出示其香港身份證，以核對身

份。完成核對身份手續後，申請人會收到一個電子證書「個人密碼信封」。

- 每份載入軟磁碟或替代存儲介質內的電子證書及私人密碼匙均由個別的「電子證書個人密碼」保護。「電子證書個人密碼」會另外以密碼信封形式分發給電子證書申請人。在隨後使用電子證書及私人密碼匙時，均需要該「電子證書個人密碼」以防範電子證書及私人密碼匙在未經準許情況下被接達。

b) 香港郵政職員會使用電腦終端機輸入申請人在申請表上提供的資料，以製作電子證書；
c) 已製作電子證書的內容會在顯示屏上展示，以便申請人核實；
d) 申請人可確認接受電子證書（見第 4.2.4 段）；確認接受電子證書的資料會傳回香港郵政系統；
e) 如申請人確認接受電子證書，申請人的電子證書及私人密碼匙會經由穩妥的機制從後端的穩妥系統內提出並存儲在軟磁碟或替代存儲介質上。載入的電子證書及私人密碼匙已由申請人密碼信封內的電子證書個人密碼保護。如申請人拒絕確認接受電子證書，其電子證書及私人密碼匙不會在香港郵政服務櫃位存儲到任何軟磁碟或替代存儲介質上；
f) 當上述程序完成後，軟磁碟或替代存儲介質會即時交給申請人；
g) 已獲接受的電子證書會在儲存庫內公佈。

4.4 證書撤銷

4.4.1 撤銷

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，香港郵政會根據在業務持續運作計劃內定明的程序迅速地撤銷所有已發出的證書（見第 4.8.2 條）。

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

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媒界，若已外洩或懷疑已外洩，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（見第 2.1.2(g) 條）。

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書面(證書撤銷通知書) 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) 認爲證書並非根據準則妥當發出；

d) 認爲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) 知道或有理由相信其資料出現在證書上之登記人：
   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、舞弊或不誠實行爲，或違反電子交易條例而在本港或海外被定罪；或
g) 認爲登記人未曾繳付登記費（見第 3.2.2 段）。

4.4.2 撤銷程序請求

登記人可透過香港郵政位於 http:www.hongkongpost.gov.hk 的指定網頁、傳真、郵寄信件、電子郵件或親身前往郵局，向香港郵政提出撤銷證書要求。香港郵政接到此要求後會“暫時吊銷證書。經登記人最後確認撤銷證書後，該證書即會撤銷且永久失效。撤銷證書之最後確認程序包括收到由登記人以其私人密碼匙進行數碼簽署之電子郵件、登記人親筆簽署之信件正本或登記人親筆簽署之撤銷證書申請表格。如未有收到登記人的最後確認，證書會繼續暫時失效，並列入證書撤銷清單，直至證書有效期屆滿爲止。撤銷證書申請表格可從香港郵政網頁 http://www.hongkongpost.gov..hk下載。香港郵政會考慮登記人的要求，把暫時吊銷的證書回復爲有效。但香港郵政只會在謹慎的情況下把暫時吊銷的證書回復爲有效。

所有被暫時吊銷或撤銷證書之有關資料（包括表明暫時吊銷或撤銷證書之原因代碼）將刊載於撤銷證書名單內。（見第 7.2 條）下次更新的證書撤銷清單不會包括由"存留"狀態回復有效的證書。

撤銷證書辦公時間如下：

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	：	上午九時至中午十二時

如懸掛八號或以上之熱帶氣旋警告信號或黑色暴風雨警告信號，且如在該日早上六時或以前信號除下，香港郵政將如常辦公；如信號在早上六時至十時之間或十時正除下，香港郵政將於該日（週六、週日或公眾假期除外）下午二時如常辦公。

4.4.3 服務承諾及證書撤銷清單更新

a) 香港郵政將作出合理努力，確保在 (1) 香港郵政從登記人處收到撤銷申請或 (2) 在無此申請之情況下，香港郵政決定暫時吊銷或撤銷證書，兩個工作日內，暫時吊銷或撤銷證書及將撤銷清單予以公佈。然而，證書撤銷清單並不會於各證書撤銷後隨即在公眾目錄中公佈。祇有在下一份證書撤銷清單更新時一併公佈，證書撤銷清單介時才會顯示該證書已撤銷之狀態。證書撤銷清單每日公佈，並存檔七年。

特此澄清，星期六、星期日、公眾假期及懸掛熱帶風暴及暴雨警報信號之工作日，一律不視作工作日計算。

香港郵政會以合理的方式，盡量在收到撤銷證書申請一星期內，透過電子郵件或以郵寄方式向有關登記人發出撤銷證書通知書。

b) 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暫時吊銷或撤銷證書後，登記人均不得在交易中使用證書。倘若或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承擔責任。

c) 此外，登記人明知香港郵政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證書人士，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，故倚據證書人士不得就交易而倚據證書。若登記人未能通知倚據證書人士，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證書人士承擔責任。

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證書人士，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。

d) 電子證書的證書撤銷清單會依據在附錄 C 內指明的時間表及格式更新。

e) 有關香港郵政對於倚據證書人仕暫時未能獲取已撤銷證書的資料時的政策，已列於本準則第 2.1.3 條(倚據證書人士之義務)及 2.2.1 條(合理技術及謹慎)

4.4.4 撤銷效力

在香港郵政把暫時吊銷 / 撤銷狀況刊登到證書撤銷清單，撤銷即終止某一證書。

4.5 電腦保安審核程序

4.5.1 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：

- 可疑網絡活動

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

4.5.2 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。

4.5.3 審核紀錄之存留期間

存檔審核紀錄文檔存留期爲七年。

4.5.4 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。

4.5.5 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)爲審核紀錄作適當備存。備存會另行離機儲存，並獲足夠保護，以免被盜用、損毀及媒體衰變。備存入檔前會保留至少一星期。

4.5.6 審核資料收集系統

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，該收集系統不能爲任何應用程式、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爲可審核事件。

4.5.7 事件主體向香港郵政發出通知

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。

4.5.8 脆弱性評估

脆弱性評估爲香港郵政核證機關保安程序之一部份。

4.6 紀錄存檔

4.6.1 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：

- 系統設備結構檔案
- 評估結果及/或設備合格覆檢(如曾進行)
- 核證作業準則及其修訂本或最新版本
- 對香港郵政具約束力而構成合約之協議
- 所有發出或公佈之證書及證書撤銷清單
- 定期事件紀錄
- 其他需用以核實存檔內容之數據

4.6.2 存檔保存期限

密碼匙及證書資料須妥爲保存七年。審核跟蹤文檔須以香港郵政視爲適當之方式存放於系統內。

4.6.3 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。

4.6.4 存檔備份程序

在有需要時製作並保存存檔之副本。

4.6.5 電子郵戳

存檔資料均註明開設存檔項目之時間及日期。香港郵政利用控制措施防止擅自調校自動系統時鐘。

4.7 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壽命爲期不超過二十年。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，相連之根源證書即會公佈供大眾取用。原先供核實用途之根源密碼匙則保留至第 4.6.2 條指定之最短之時限，以便日後核對用原先密碼匙進行之簽署。

4.8 災難復原及密碼匙資料外洩計劃

4.8.1 災難復原計劃

香港郵政已備有妥善管理之程序，包括每天爲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設施不少於十千米。業務持續運作計劃每年均會檢討及執行。

如發生嚴重故障或災難，香港郵政會即時知會資訊科技署署長，並公佈運作由生產基地轉至災難復原基地。

在發生災難後但穩妥可靠的環境尚未重新確立前：

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

4.8.2 密碼匙資料外洩計劃

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

如根據本準則簽發電子證書的私人密碼匙資料外洩，香港郵政會即時知會資訊科技署署長並作出公佈。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。

4.8.3 密碼匙的替補

倘若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資訊科技署署長並作出公佈。公佈內容包括已撤銷證書的名單、如何在香港郵政本身的公開密碼匙已撤銷的情況下、爲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。

4.9 核證機關終止服務

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”所定程序知會資訊科技署署長並作出公佈。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。

5． 實體、程序及人員保安控制

5.1 實體保安

5.1.1 選址及建造

香港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，爲核證機關運作作好準備。

5.1.2 進入控制

香港郵政實施商業上具合理實體保安之控制，限制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）。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人手或電子監控，以防發生未經授權入侵。

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 自然災害

核證機關設施在合理可能限度內受到保護，以免受自然災害影響。

5.1.5 防火及保護

香港郵政已爲核證機關設施備妥防火計劃及滅火系統。

5.1.6 媒體存儲

媒體存儲及處置程序已經開發備妥。

5.1.7 場外備存

香港郵政核證系統數據的適當備存會作場外儲存，並獲足夠保護，以免被盜用、損毀及媒體衰變。（另見第 4.8.1 條）

5.1.8 保管印刷文件

印刷文件及身分確認文件之影印本由香港郵政妥爲保存。獲授權人員方可以取閱該等紀錄。

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。

香港郵政已爲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
- 職責劃分

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

5.3 人員控制

5.3.1 背景及資格

香港郵政採用之人員及管理政策可合理確保其人員，包括僱員、承包商及顧問之可信程度及勝任程度，並確保他們以符合本準則之方式履行職責及表現令人滿意。

5.3.2 背景調查

香港郵政對擔任受信職責之人員進行調查（其受聘前及其後有需要時定期進行），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。

5.3.3 培訓要求

香港郵政人員已接受履行其職責所需要之初步培訓。有需要時香港郵政亦會提供持續培訓，使人員能掌握所需最新工作技能。

5.3.4 向人員提供之文件

香港郵政人員會收到綜合用戶手冊，詳細載明證書之製造、發出、更新、續期及撤銷程序及與其職責有關之其他軟件功能。

6． 技術保安控制

本條說明香港郵政特別爲保障加密密碼匙及相關數據所訂之技術措施。控制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、使用及毀滅核證機關證書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

除非程序被授權用戶外洩，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私人密碼匙的獲授權用戶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。

6.1.2 登記人公開密碼匙交付

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的配對密碼匙。

6.1.3 公開密碼匙交付予登記人

用於核證機關數碼簽署之各香港郵政配對密碼匙之公開密碼匙可從網頁 http://www.hongkongpost.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 密碼匙大小

香港郵政之簽署配對密碼匙爲 2048 位元 RSA。登記人配對密碼匙則爲 1024 位元 RSA。

6.1.5 加密模組標準

香港郵政進行之簽署產生密碼匙、存儲及簽署操作在硬件加密模組進行。

6.1.6 密碼匙用途

香港郵政電子證書(個人)使用之密碼匙可用於數碼簽署以及加密電子通訊。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

6.2.1 加密模組標準

香港郵政私人密碼匙利用加密模組產生，其級別至少達到 FIPS 140-1 第 3 級。

6.2.2 私人密碼匙多人式控制

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作啓動、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爲香港郵政私人密碼匙及登記人私人密碼匙設計整體性密碼匙托管程序。有關香港郵政私人密碼匙的備存，見第 6.2.4 條。

6.2.4 香港郵政私人密碼匙備存

香港郵政私人密碼匙的備存，是使用達到 FIPS 140-1 第 2 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啓動。其他私人密碼匙均不設備存。所有私人密碼匙不會存檔。

6.3 配對密碼匙管理其他範疇

香港郵政之核證機關密碼匙使用期不超過二十年（見第 4.7 段）。所有香港郵政密碼匙之產生、銷毀、儲存以及證書及撤銷清單簽署運作程序，均於硬件加密模組內進行。第 4.6 條詳述香港郵政公開密碼匙紀錄存檔之工作。

6.4 電腦保安控制

香港郵政實行多人控制措施，控制啓動數據（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。此等保安控制措施接受第 2.6 條遵守規定之審核。

6.5 生命週期技術保安控制

香港郵政控制爲香港郵政系統購置及發展軟件及硬件之程序。現已定下更改控制程序以控制並監察就香港郵政系統部件所作的調整及改善。

6.6 網絡保安控制

香港郵政系統有防火牆以及其他接達控制機制保護，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。

6.7 加密模組工程控制

香港郵政使用之加密裝置至少達到 FIPS140-1 第 2 級。

7． 證書及證書撤銷清單結構

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）。本準則提及之證書一律以 X.509 第三版本之格式發出。（見附錄 B）。附錄 D 載有各類香港郵政電子證書之特點摘要。

7.2 證書撤銷清單結構

香港郵政證書撤銷清單之格式爲 X.509 第二版本（見附錄 C）。

8· 準則管理

更改本準則一律須經香港郵政核准及公佈。有關準則一經香港郵政在網頁http://www.hongkongpost.gov.hk或香港郵政儲存庫公佈，更改即時生效，並對證書新申請人以及爲現有證書續期的登記人均具約束力。就任何對本準則作出的更改，香港郵政會實際可行地盡快通知資訊科技署署長。申請人、登記人及倚據證書人士可從香港郵政網頁http://www.hongkongpost.gov.hk或香港郵政儲存庫瀏覽此份準則以及其舊有版本。

附錄 A - 詞彙

除非文意另有所指，否則下列文詞在本準則中釋義如下：

“申請人”指自然人或法人並已申請電子證書。

“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。

“證書”或**“電子證書”**指符合以下所有說明之紀錄 ：

a) 由核證機關爲證明數碼簽署之目的而發出而該數碼簽署用意爲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) 經發出紀錄核證機關之負責人員簽署。

“核證機關”指向他人(可以爲另一核證機關)發出證書者。

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

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

“對應”就私人或公開密碼匙而言，指屬同一配對密碼匙。

“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。

“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、數目字或其他符號爲認證或承認該紀錄之目的定立或採用者。

“身份證”指由香港特別行政區政府入境事務處，根據人事登記（修訂）條例發出的香港身份證，包括智能身份證。

“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，指核證機關製造證書並將該證書之內容通知該證書內指名或識別爲獲發給該證書之人之行爲。

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

"條例"指香港法例第 553 章電子交易條例。

"發訊者"就某電子紀錄而言，指發出或產生該紀錄者，或由他人代爲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) 根據第 22 條認可之證書；
(b) 屬根據第 22 條認可之證書之類型、類別或種類之證書；或
(c) 第 34 條所述核證機關所發出指明爲認可證書之證書。

"認可核證機關"指根據第 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。

"倚據限額"指就認可證書倚據而指明之金錢限額。

"儲存庫"指用作儲存並檢索證書以及其他與證書有關資訊之資訊系統。

"負責人員"就某核證機關而言，指在該機關與本條例有關活動中居要職者。

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

"智能身份證"指可將電子證書載入其中的**身份證**。

"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爲獲發給證書；
(ii) 已接受該證書；及
(iii) 持有與列於該證書內的公開密碼匙對應之私人密碼匙；

"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) 依循廣爲接受之安全原則。

爲執行電子交易條例，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，而該證書之登記人爲簽署人，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

		電子證書（個人）證書	**發出予未滿18歲人仕的 電子證書（個人）**
標準欄 (Standard field)			
版本 (Version)		X.509 V3	
序號 (Serial number)		[由香港郵政系統設置]	
簽署算式識別 (Signature algorithm ID)		sha1RSA	
發證人 (Issuer)		cn=Hongkong Post e-Cert CA 1, o=Hongkong Post, c=HK	
有效期 (Validity period)	**不早於 (Not before)**	[由香港郵政設置的UTC 時間]	
	不遲於 (Not after)	[由香港郵政設置的UTC 時間]	
主體名稱 (Subject name)		cn=[香港身份證姓名]（附註1）， e=[電子郵箱地址]（附註2） ou=[登記人參考編號]（附註3）， o=Hongkong Post e-Cert (Personal), c=HK	cn=[香港身份證姓名]（附註1）， e=[電子郵箱地址]（附註2） ou=[登記人參考編號]（附註3） o=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)：密碼匙長度爲1024-bit	
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 1, o=Hongkong Post, c=HK	
	序號 (Serial number)	[從發出人處獲取]	
密碼匙的使用 (Key usage)		不可否認，數碼簽署，密碼匙加密 **此欄爲「關鍵欄」**	
證書政策 (Certificate policy)		PolicyIdentifier = 1.3.6.1.4.1.16030.1.1.2（附註 6） PolicyQualifierID = CPS Qualifier = [核證作業準則的URL]	
主體其他名稱 (Subject alternative name)	**DNS**	[經加密的香港身份證號碼]（附註7）	
	rfc822	[證書持有人電子郵箱地址]（附註2）	
發證人其他名稱 (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 constraints)	無	
延伸密碼匙的使用 (Extended key usage)		未使用	

		電子證書（個人）證書	**發出予未滿18歲人仕的 電子證書（個人）**
證書撤銷清單分發點 (CRL distribution point)		**分發點名稱 = [證書撤銷清單分發點URL]**（附註8）	
Netscape 延伸欄位 (Netscape extension)（附註5）			
Netscape 證書類型 (Netsacpe cert type)		SSL client, S/MIME	
Netscape SSL伺服器名稱 (Netscape SSL server name)		未使用	
Netscape 備註 (Netscape comment)		未使用	

附註:

1. 申請人姓名格式: 英文格式 - 姓氏（大寫）+ 名 （例如 CHAN Tai Man David）
2. 申請人電子郵箱地址（選項）
3. 登記人參考編號： 10 位數字
4. “e-Cert (Personal/Minor)” 表示 申請人於遞交證書申請表時未滿 18 歲（見本核證作業準則第 3.1.1.2 段）.
5. 除非另外註明，所有標準延伸欄位及 Netscape 延伸欄位均爲 “非關鍵” (Non-Critical) 延伸欄位。
6. 香港郵政已獲 Internet Assigned Numbers Authority (IANA) 分配私人企業號碼 (Private Enterprise Number) 16030 號。「1.3.6.1.4.1.16030.1.1.2 」爲本準則的物件識別碼 (Object Identifier, OID)。
7. 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爲一雜湊數值(以 cert_hkid_hash 表示)後，存入證書：

   cert_hkid_hash = *SHA-1* ($RSA_{privatekey,\ sha\text{-}1}$ (hkid_number))

   *SHA-1*爲一雜湊函數而*RSA*則爲簽署函數

   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 $SHA\text{-}1\ (\ RSA_{privatekey,\ sha\text{-}1}\ (\ \text{hkid\_number}\ )\ )$。該雜湊數值會輸入證書內的指定延伸欄位。
8. 證書撤銷清單分發點 URL 爲 http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL1_<xxxxx>.crl, 其中 <xxxxx> 爲經香港郵政系統產生，包含 5 個數字或字符的字串。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。

附錄 C - 香港郵政電子證書撤銷清單(CRL)格式

就根據本核證作業準則而發出的電子證書而言，香港郵政每天三次更新及公佈下述的證書撤銷清單（更新時間爲香港時間 09:15、14:15 及 19:00（即格林尼治平時[GMT] 時間 01:15、06:15 及 11:00））：

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。公眾可於在證書的「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「分割式證書撤銷清單」。該位址(URL)會以下述方式表示：

http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL1_<xxxxx>.crl

其中 <xxxxx> 爲 經香港郵政系統產生，包含 5 個數字或字符的字串

b) **「整體證書撤銷清單」**(Full CRL) 包含所有已暫時吊銷或已撤銷證書的資料。公眾可於位址(URL)獲取「整體證書撤銷清單」：

http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL1.crl;或
ldap://ldap1.hongkongpost.gov.hk (port 389, cn=Hongkong Post e-Cert CA 1 CRL1, o=Hongkong Post, c=HK)。

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（見本準則第 2.5 段）。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。

分割式及整體證書撤銷清單格式:-

標準欄位 (Standard field)	子欄位 (Sub-field)	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爲 X.509 第二版
簽署算式識別 (Signature algorithm ID)		sha1RSA		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 1 O=Hongkong Post 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]		此欄列出已撤銷的證書並以證書序號排列次序
	撤銷日期	[UTC 時間]		此欄顯示撤銷證書的日期

標準欄位 (Standard field)	子欄位 (Sub-field)	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
	(Revocation date)			
	輸入證書撤銷清單資料申延欄位 (CRL entry extensions)			
	原因代碼 (Reason code)	[撤銷理由識別碼]		（附註 1）
標準延伸欄位 (Standard extension)（附註 2）				
機關密碼匙識別名稱 (Authority key identifier)	發出人 (Issuer)	CN=Hongkong Post Root CA 1 O=Hongkong Post 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]		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)] **本欄位爲"關鍵"欄位**	[未使用]	本欄位祇爲分割式證書撤銷清單使用。

附註：

1. 以下爲可於撤銷證書欄位下列出的理由識別碼：

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

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

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

附錄 D - 香港郵政電子證書 – 服務摘要

要點	***電子證書(個人)***	***發出予未滿 18 歲人仕的電子證書(個人)***
申請人/ 登記人	持有香港身份證及於遞交證書申請表時年滿 18 歲人仕	持有香港身份證及於遞交證書申請表時未滿 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	1024-bit RSA	
產生配對密碼匙	由香港郵政代製產生	
核對身份	當面核對申請人的身份，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	
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)； 電子郵箱地址；及 登記人參考編號（由香港郵政系統產生）	
登記費用（見本準則第 2.4 段）	每份證書（包括首次及續期申請）每年 50 港元	
證書有效期	三年（附註 1）	

附註

1. 根據證書續期程序而發出之證書有效期可超過三年，但不會超過三年另一個月（見本核證作業準則第 1.2.4 及 3.3 段）