以香港郵政署長
根據電子交易條例作為認可核證機關
之
電子核證證書（e-Cert）
核證作業準則

日期：二〇〇二年五月二十七日

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為：經公開密碼匙加密之信息只可用其配對私人密碼匙解密；和經私人密碼匙加密之信息亦只可用其配對公開密碼匙解密。

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

根據條例所載規定，就條例及公匙基建而言，香港郵政署長為認可核證機關。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，其身分為香港郵政。

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、撤回及利用公開儲存庫公佈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。此等證書稱為“證書”或“電子核證證書”。香港郵政發出證書予個人（“電子核證(個人)證書”）、機構（“電子核證(機構)證書”）及欲以其伺服器名稱獲發證書之機構（“電子核證(伺服器)證書”）。此外，香港郵政尚為某些機構發出用以加密電子通訊之證書（“電子核證（保密）證書”）。

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 – 香港郵政電子核證證書格式
附錄 C – 香港郵政電子核證證書撤銷清單格式
附錄 D – 香港郵政電子核證證書特點摘要

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、撤回及公佈證書時採用之做法及標準。

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

除電子核證（保密）證書（見第 1.2.3(d)條）外，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，香港郵政為認可核證機關。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認可及接受之數碼證書。換言之，香港郵政指定為認可證書者均為認可證書，而其內容不但準確，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）。

附錄 D 載有香港郵政電子核證證書特點摘要

1.2 社區及適用性

1.2.1 核證機關

根據本準則，香港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，即表明該證書得到完全及最終確認。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。登記人乃已取得發出香港郵政電子核證之個人或機構。倚據證書人士乃已接受香港郵政電子核證以用於交易之實體。接受其他登記人之香港郵政電子核證證書以用於交易之登記人乃為有關此證書之倚據證書人士。請倚據證書人士留意。香港郵政電子核證並無年齡限制，故未成年人可申請並領取證書。倚據證書人士不得用電子核證作為電子核證登記人之年齡證明。

1.2.2.1 登記人之保證及陳述

各登記人（如申請電子核證（機構）證書、電子核證（伺服器）證書或電子核證（保密）證書，獲授權代表會代表登記人機構）須簽署一份協議（按本準則規定之條款），其中載有一條款，登記人據此條款同意，登記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、電子核證（機構）證書授權用戶及電子核證（保密）證書授權單位外，並無其他人士曾取用登記人之私人密碼匙；**
b) **使用與登記人電子核證（個人）證書、電子核證（機構）證書或電子核證（伺服器）證書所載之公開密碼匙相關之登記人私人密碼匙所產生之每一數碼簽署實屬登記人之數碼簽署。**
c) **電子核證（保密）證書只可根據下列第** 1.2.3(d)**條列明的用途而使用。**
d) **證書所載之所有資料及由登記人作出之陳述均屬真實。**
e) **證書將只會用於符合準則之認可及合法用途。**
f) **在證書申請過程中所提供之所有資料，均並無侵犯或違反任何第三方之商標、服務標記、品牌、公司名稱或任何知識產權。**

1.2.3 登記人之類別

根據本準則香港郵政僅發出證書予其申請已獲批准並已適當形式簽署登記人協議之申請人士。根據本準則和登記人協議，四類證書會予以發出。

a) 電子核證（個人）證書

第一類證書發給持有香港身份證之人士。此等證書可用來從事商業經營。電子核證（個人）證書可發出予持有香港身份證之十八歲以下人士，惟該等人士之父母中之一人（或合法監護人）須成為有關登記人協議之一方。向未成年人發出之電子核證（個人）證書可載有對倚據證書人士之特別警示，因為根據法律規定，未成年人可能不受若干合約約束。

b) 電子核證（機構）證書

第二類證書發給香港特別行政區政府各局及部門、獲香港特別行政區政府簽發有效商業登記證之機構以及獲香港法例認可之本港法定團體，並識別機構已決定應具有表明成員或僱員與機構關係之證書之機構成員或僱員。此等證書與電子核證（個人）證書之用途大致相同。

c) 電子核證（伺服器）證書

第三類證書發給擬擁有以伺服器名義發出之證書之香港特別行政區政府各局及部門、獲政府簽發有效商業登記證之機構以及獲香港法例認可之本港法定團體。

d) 電子核證（保密）證書

第四類證書發給香港特別行政區政府各局及部門、獲香港特別行政區政府簽發有效商業登記證之機構以及獲香港法例認可之本港法定團體。證書擬供已獲登記人機構授權使用證書之該機構單位（“授權單位”）使用。

此類證書只可用作：

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

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

此外，此類證書產生之數碼簽署只可用作認收電子信息，並只可用於與聯機付款或聯機投資無關或不相連或不會聯機為任何人士或實體帶來任何性質之財務利益之交易。不論任何情況，此等證書產生之數碼簽署均不得用作認收與洽商或訂定合約或任何具法律效力之協議有關而傳送之電子信息。

1.2.4 證書之期限

根據本核證作業準則發出之證書有效期為一年。(見第 3.2 條證書續期)

1.2.5 在香港郵政署所進行個人申請

對於所有首次申請及證書撤銷或到期後之申請，申請人須親身前往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，呈交所須之鑑別文件、申請表格及已簽署之登記人協議（如適用），並應回答有關上述文件之問題。就電子核證（個人）證書而言，此表明該等證書之所有申請人均須親身呈遞（十八歲以下申請人之父母或合法監護人除外）。就電子核證（機構）證書而言，擬名列證書之成員或僱員無需親身呈遞，但其機構獲授權代表則須親身呈遞。就電子核證（伺服器）證書而言，此表明作出申請之機構獲授權代表須親身呈遞。申請人親身呈遞時，將須出示

身分證明。（另見下文第 3 條）。

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 號香港郵政電子服務科
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。無論登記人是否亦為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，香港郵政為認可核證機關，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。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) 通知登記人有關被拒絕的申請（見第 4.1 條），
c) 通知登記人有關已批準的申請及如何提取證書（見第 4.2 及 4.3 條），
d) 撤銷證書及依時公佈證書撤銷清單（見第 4.4 條），
e) 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（見附錄 D）負責：

a) 若不需要香港郵政　其提供代製密碼匙服務，則在獲取證書之過程中使用穩當系統以安全方法產生配對密碼匙。倘若香港郵政　登記人提供代製密碼匙服務，香港郵政將代表登記人，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，以保證私人密碼匙不受干擾。
b) 適當完成申請程序並在適當表格內簽署登記人協議（如申請電子核證（機構）證書、電子核證（伺服器）證書或電子核證（保密）證書，則由獲授權代表簽署）；履行該協議規定其應承擔之義務及確保在申請證書時所作的陳述準確無誤。
c) 若不需要香港郵政　其提供代製密碼匙服務，則完成由香港郵政發出之證書，包括按照遵循電子核證客戶套件及附連唯讀光碟（或替代存儲介質）所載關於完成證書之指示。
d) 承認其透過接受證書（其於完成證書過程中將作出）而承諾使用合理預防措施來保護其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) 若屬電子核證（保密）證書，則保證：
    - 授權用戶只獲登記人機構授權使用證書以及有關之數碼簽署，以解密並認收對方送來加密之電子信息，不得作其他用途；
    - 此等證書只可用以(i)向登記人傳送加密電子信息，(ii)容許登記人機構為信息解密，以及(iii)容許登記人機構發出認收信息並附加其數碼簽署以證實其登記人機構收件身分，藉此確認送出之加密信息已經收訖。
    - 不會試圖使用電子核證（保密）證書的私人密碼匙以產生數碼簽署並用作認收信息以外用

途。

- 授權用戶採取合理預防措施以維護私人密碼匙之安全。

f) 發現其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）。

g) 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。

h) 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。

i) 同意其透過接受證書而向香港郵政保證（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。

j) 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香港郵政知會，香港郵政擬根據本準則之條款暫停或撤銷證書後，均不得在交易中使用證書。

k) 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，因情形乃屬如此，故倚據證書人士不得就交易而倚據證書。

2.1.2.1 登記人之責任

各登記人（見附錄 D）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

倚據香港郵政電子核證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；且若屬電子核證（保密）證書，更須考慮倚據本準則所載明之規定該證書之用途有限。

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各倚據證書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登記人協議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，若登記人作為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偽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為。

2.2.2 非商品供應

特此澄清，登記人協議並非任何性質商品之供應合約。任何及所有據此發出之證書持續為香港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，登記人僅有權促致證書發出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證書人士接達之公開儲存庫內提供之證書，並非作為對倚據證書人士供應任何商品；亦不會作為對倚據證書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；亦不會作為向倚據證書人士作出供應商品的陳述或保證。唯一不在此限者，為下文第 4.3 條所指之電子核證客戶套件及唯讀光碟（或替代存儲介質）。此等物品之擁有權或利益不得轉讓予登記人。香港郵政雖同意將上述物品免費轉讓予登記人作下文第 4.3 條指定用途，但亦承諾合理謹慎確保此等物品適合作下文第 4.3 條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，唯讀光碟（或替代存儲介質）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，而須由唯讀光碟（或替代存儲介質）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為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

在香港郵政違反本登記人協議或任何謹慎職責，尤其就登記人而言，當登記人或其他人或以其他任何方式倚據香港郵政根據此公開密碼匙基礎建設發出之任何證書時根據本登記人協議香港郵政違反其應合理採取技術或謹慎及/或職責之條款之情況下, 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證書人士，登記人蒙受損失及損害，香港郵政概不負責關乎下述原因之賠償或其他補救措施：(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，香港郵政已獲提前通知此類損失或損害之可能性。

2.2.3.3 限額 -- 50 萬港元及 25 萬港元

除下文所述例外情況外，在香港郵政違反本登記人協議或任何謹慎職責，尤其就登記人而言，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香港郵政根據此公開密碼匙基礎建設發出之任何證書時香港郵政違反根據本準則其應合理採取技術或謹慎及/或職責之條款之情況下，登記人或倚據證書人士蒙受損失及損害（無論作為根據準則或以其他任何方式定義之登記人或倚據證書人士），香港郵政對任何登記人或任何倚據證書人士（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證書人士或以任何其他身分）所負法律責任限制於且任何情況下不得超過每份個人證書、機構證書或伺服器證書 50 萬港元，或每份保密證書 25 萬港元。

2.2.3.4 提出索償之時限

任何登記人因（無論擬作為登記人或倚據證書人士）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，則應在登記人清楚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、僱員或代理人均不會自願接受或均不會接受向登記人擔負其任何個人出於真誠以任何方式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所做任何作為或不作為相關之謹慎責任或職責；各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）以任何方式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所作任何行動或不行動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 蓄意之不當行為或個人傷亡之責任

任何因欺詐或蓄意之不當行為或個人傷亡之責任均不在本準則、登記人協議或香港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 消費者之責任

有關非為經營業務而訂定登記人協議之登記人或訂約時並無表明為經營業務為目的者，在法律上，因香港郵政未能以合理技術及謹慎履行本登記人協議而原本適用之部分或全部法律責任限制條款有可能不適用於此類登記人之申索。

2.2.3.8 證書通知、限制及倚據限額

香港郵政發出之證書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為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。

倘閣下為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為 0 港元。

若本證書在任何方面不準確或誤導，而該等不準確或誤導乃因香港郵政署長、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50 萬港元，或若屬電子核證（保密）證書，向每名倚據證書人士支付最多25 萬港元，惟該等損失不屬於及不包括（1）任何直接或間接利潤或收入損失、信譽或商譽損失或傷害、任何商機或契機、失去工程或失去或無法使用任何數據、設備或軟件或（2）任何間接、相應而生或附帶引起之損失或損害，而且即使在後者情況下，香港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為50 萬港元，或若屬電子核證（保密）證書，則為25 萬港元，而在所有情形下就第（1）及（2）類損失而言倚據限額則為0 港元。

在任何情況下，香港郵政署、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 香港郵政對已接受但有缺陷之電子證書或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，假如下文第** 3.1.7 **條或** 4.3 **條所述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。**

2.2.4.2 **儘管上文已列明香港郵政承擔責任之限制，若登記人接獲證書後發現，因電子核證(個人)、電子核證(機構)及電子核證(伺服器)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，而使用電子核證(保密)證書時，則保密電子通訊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 登記人轉讓

登記人不可轉讓登記人協議或證書賦予之權利。擬轉讓之行為均屬無效。

2.2.6 陳述權限

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，登記人及倚據證書人士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，直至該等條款成為合法及可執行為止，同時應保留該等條款之本意。本準則之任何條款之不可執行性將不損害任何其他條款之可執行性。

2.3.3 爭議解決程序

香港郵政關於本準則範圍內之事宜之決定為最終決定。香港郵政將不就登記人或倚據證書人士之爭議採取任何其他爭議解決程序。如有索償，請送交下列地址：

香港中環康樂廣場 2 號
香港郵政電子服務科
電子地址：enquiry@hongkongpost.gov.hk

2.3.4 詮釋

本準則中英文本措詞詮釋若有歧異，則以英文本為準。

2.4 收費

每份電子核證(個人)證書（包括首次及續期申請）年費為 50 港元。

每份電子核證(機構)證書首次申請年費為 50 港元，續期年費則為 150 港元。此外，每份申請，不論授權用戶數目多少，均須另繳交行政費 150 港元。

每份電子核證(伺服器)證書（包括首次及續期申請）年費為 2,500 港元。

每份電子核證（保密）證書（包括首次及續期申請）年費為 150 港元。此外，每份申請，不論授權單位數目多少，均須另繳交行政費 150 港元。

2.5 公佈資料及儲存庫

香港郵政維持一儲存庫，內有簽發證書清單一份、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核證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。香港郵政每次處理批核證書申請後，即時會在儲存庫公佈根據本準則發出之證書。香港郵政儲存庫可透過 URL ldap://ldap.hongkongpost.gov.hk.及 http://www.hongkongpost.gov.hk/crl/eCert.crl 接達。

2.5.1 證書儲存庫控制

儲存庫所在位置可供網上瀏覽，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

每份證書一經發出或第 4 條所述之相關情況一旦發生，儲存庫均會即時更新。

2.6 遵守規定之審核

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審核，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

此條限制適用於香港郵政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。作為根據本準則申請電子核證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登記人資料，惟根據香港法例無法追溯個別人登記人之綜合資料除外不在此限。

3． 鑑別及認證

3.1 首次登記

除非申請人為電子核證(機構)證書之申請人，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、3.1.9 及 3.1.10 條所述身分證明。如申請人為在電子核證(機構)證書上列明之申請人，則無須親身呈遞，但該申請機構之獲授權代表須親身呈遞。

所有證書申請人須向香港郵政呈交一份填妥並經簽署之申請表及登記人協議。電子核證(機構)、(伺服器)及(保密)證書之申請表亦須經申請人所屬機構獲授權代表填妥及簽署，並要求申請機構成為登記人(另見第 3.1.1.5 條)。申請獲承認後，香港郵政即準備證書並向申請人發出通知，說明如何檢索證書。

3.1.1 名稱類型

3.1.1.1 電子核證(個人)證書

透過證書上登記人名稱可識別電子核證(個人)證書登記人之身分，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。
b) 以雜湊數值形式把登記人的香港身份證號碼儲存於證書內 (見附錄 B)。

3.1.1.1.1 向十八歲以下登記人士簽發電子核證(個人)證書

此等登記人識別方法同上，其父母或合法監護人雖然須為登記人，但其名稱不會在證書顯示。

3.1.1.2 電子核證(機構)證書

透過證書上登記人名稱可識別電子核證(機構)證書登記人機構之身分，該名稱由以下資料組成：

a) 授權用戶香港身份證/護照上顯示之申請人姓名；
b) 登記人機構在有關香港政府部門或登記機關之登記名稱或獲香港法例認可之本港法定團體名稱；如登記人機構為香港特別行政區政府部門或局，則為該部門或局之正式名稱；及
c) 若登記人機構並非香港特別行政區政府部門或局或香港法例認可之法定團體，則包括該機構之香港公司註冊/商業登記號碼。

3.1.1.3 電子核證(伺服器)證書

透過證書上登記人名稱可識別電子核證(伺服器)證書登記人機構之身分，該名稱組成為：

a) 登記人機構在有關香港政府部門或登記機關之登記名稱或獲香港法例認可之本港法定團體名稱；如登記人機構為香港特別行政區政府部門或局，則為該部門或局之正式名稱；
b) 若登記人機構並非香港特別行政區政府部門或局或香港法例認可之法定團體，則包括該機構之香港公司註冊/商業登記號碼；及
c) 登記人機構所擁有伺服器（包括網域名稱）之名稱。

3.1.1.4 電子核證（保密）證書

透過證書上登記人名稱可識別電子核證（保密）證書登記人機構之身分，該名稱組成為：

a) 登記人機構在有關香港政府部門或登記機關之登記名稱或獲香港法例認可之本港法定團體名稱；如登記人機構為香港特別行政區政府部門或局，則包括該部門或局之正式名稱；
b) 若登記人機構並非香港特別行政區政府部門或局或香港法例認可之法定團體，則包括該機構之香港公司註冊/商業登記號碼；及
c) 登記人機構內登記單位之名稱。

3.1.1.5 獲授權代表

機構獲授權代表雖替登記人機構辦理電子核證（機構）、（伺服器）或（保密）證書申請手續，然而該證書並不會辨識此獲授權代表身分。

3.1.1.6 機構中文名稱

電子核證證書一律只用英文簽發，因此只有中文名稱或只提供中文名稱作登記之機構，其名稱不會顯示在證書上。雖然如此，登記人仍可按網頁 http://www.hongkongpost.gov.hk之指示搜尋機構之中文名稱。

3.1.2 名稱需有意義

所採用名稱之語義必須為一般人所能理解，方便辨識登記人身分。

3.1.3 詮釋各個名稱規則

香港郵政電子核證證書會載入之登記人名稱(主體名稱)類型見第 3.1.1 條。有關香港郵政電子核證證書主體名稱之詮釋應參照附錄 B。

3.1.4 名稱獨特性

登記人名稱所有部分(包括登記人參考編號)合而為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

香港郵政對可酌情處理有關名稱爭議之事宜，其決定為最終決定。

3.1.6 認證及商標之作用

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

a) **由登記人產生其配對密碼匙**

登記人須產生其配對密碼匙，並使用穩當系統執行此項工作。登記人均承認，須為維持與證書中公開密碼匙相關之私人密碼匙之保安承擔全部責任。香港郵政系統在接獲登記人要求產生證書之要求後，會核對裝有公開密碼匙之證書要求架構所載的簽署，查清對方確實擁有該私人密碼匙。

b) **代製密碼匙服務**

倘若香港郵政為登記人提供代製密碼匙服務，香港郵政將在其處所內使用穩當的系統，在安全的環境下替登記人製作證書，以保證私人密碼匙不受干擾。私人密碼匙連同證書將被存儲在軟碟上，並以申請表中指明的安全方式交付予登記人。香港郵政全面保留權力，當有合適的技術可以利用時，可用技術可行的其他存儲介質代替軟碟，保存私人密碼匙及證書。若使用技術可行的其他存儲介質，其仍會以申請表中指明的安全方式交付予登記人。

3.1.8 機構身分認證

接獲電子核證(機構)證書申請時，香港郵政會根據第 3.1.9 條簡列之程序認證登記人身分。只有獲授權代表須完成下文簡列親身呈遞申請手續，並出示：（1）註明該機構已授權有關人士 (即「獲授權代表」)代表該機構提交申請的授權書及識別列於電子核證(機構)證書上的授權用戶，授權書上須蓋上該機構"For and on behalf of "(代表機構簽署)印章及附有該機構的獲授權簽署；(2）所有按此方式識別身分之授權用戶之香港身份證及護照副本以及獲授權代表本人之香港身份證及護照以及（3）由有關香港登記機關發出證明此機構確實存在之文件。

電子核證（伺服器）證書必須經由登記人機構獲授權代表親身前往指定之香港郵政處所或其他已獲香港郵政指定之機構處所，遞交申請。獲授權代表須出示（1）註明該機構已授權有關人士 (即「獲授權代表」)代表該機構提交申請並證明伺服器證書所載網域名稱擁有權的授權書，授權書上須蓋上該機構"For and on behalf of" (代表機構簽署)印章及附有該機構的獲授權簽署；(2）獲授權代表本人香港身份證或護照及（3）由有關香港登記機關發出證明此機構確實存在之文件。

電子核證（保密）證書必須經由登記機構獲授權代表親身前往指定之香港郵政處所或其他已獲香港郵政指定之機構處所遞交申請。獲授權代表須出示（1）註明該機構已授權有關人士 (即「獲授權代表」)代表該機構提交申請的授權書，授權書上須蓋上該機構"For and on behalf of" (代表機構簽署)印章及附有該機構的獲授權簽署；(2）獲授權代表本人香港身份證或護照及（3）由有關香港登記機關發出證明此機構確實存在之文件。

香港特別行政區政府各局或部門如欲提出申請，獲授權代表亦須親身前往指定之香港郵政處所或其他獲香港郵政指定之機構處所，遞交蓋上該局或部門印鑑之便箋、信函或有關申請表格，信中須指定該員已為獲授權代表，可代表該局或部門簽署與申請、撤銷及續發香港郵政證書有關之所有文件。便箋、信函或有關申請表格須由部門秘書或同級人員簽署。

3.1.9 個人身分認證

各個人登記人身分之確認將透過如下運作之親身呈遞過程得以完成：

各證書申請人須親身到指定之香港郵政處所或其他已獲香港郵政指定之機構處所，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。該前述處所人員將保留其身份證影印本一份，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。

3.1.10 十八歲以下登記人個人身分認證

十八歲以下（未成年人）各申請人須親身到指定之香港郵政處所或其他已獲香港郵政指定之機構處所，出示（1）填妥並已簽署（由將要成為登記人之未成年人及其父母或監護人簽署）之申請表及登記人協議（2）該未成年人之出生證書（3）將要成為登記人之未成年人之香港身份證，及其父母或合法監護人之香港身份證或護照之副本（4）若屬合法監護人情況，提交此監護人身分之正式文件。

3.2 證書續期

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、已吊銷或已撤銷的證書續期。香港郵政會於證書的有效期屆滿前以電子郵件向登記人發出續期通知。

3.2.1 電子核證(個人)證書

每一電子核證(個人)證書可續期而無須如首次申請時般進行面對面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。一經續期，登記人可透過香港郵政的代製密碼匙服務來 生配對密碼匙；倘若登記人在申請續期時提出要求，亦可透過類似首次申請時之電子互動過程產生新配對密碼匙。續期以後，只要登記人協議原有之條款及條件與續期當日有效的核證作業準則條款並無抵觸，則原訂的條文仍適用於新續期之證書。如兩者有所抵觸，則以續期當日之核證作業準則內的條款為準。申請人應細閱續期當日有效的核證作業準則，方可遞交續期申請表。

3.2.2 電子核證(機構)證書、電子核證(伺服器)證書及電子核證(保密)證書

電子核證(機構)證書、電子核證(伺服器)證書及電子核證(保密)證書不會自動續期。若香港郵政接收到續期申請，即會根據 3.1.8 條所述“機構身分認證”之過程重新進行認證。機構的獲授權代表須填妥證書續期申請表(可於香港郵政網址 http://www.hongkongpost.gov.hk 下載)，並連同申請書內列明的其他文件以及續期費用，一併交回。如獲授權代表人選有變，獲授權代表亦須填妥並簽署登記人協議，一併交回香港郵政。續期以後，只要登記人協議原有之條款及條件與續期當日有效之核證作業準則條款並無抵觸，則原訂的條文仍適用於新續期的證書。如兩者有所抵觸，則以續期當日之核證作業準則內的條款為準。申請人應細閱續期當日有效的核證作業準則，方可遞交續期申請表。

4. 運作要求

4.1 證書申請

按本準則申請證書之申請人必須填妥香港郵政編定之表格，提交申請。有關用以確定登記人身份所需文件，可參閱本準則第 3.1.8 條（機構身分認證）、第 3.1.9 條（個人身分認證）及第 3.1.10 條（十八歲以下登記人個人身分認證）。為使登記人取得新證書而向登記人提供的資訊，可參閱本準則第 4.3 條及登記人協議。登記人須於提交證書申請時一并提交已簽署的登記人協議。申請人與香港郵政經電子傳送之所有申請資料須使用由香港郵政訂明之安全接層(Secure Socket Layer)或某一類似規約。

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 製造及發出證書

a) **由登記人產生其配對密碼匙**

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。證書發出程序如下：

- 申請人在其裝置產生私人密碼匙及公開密碼匙。
- 公開密碼匙會載於要求發出證書之信息內，信息會傳送至香港郵政。接到要求發出證書之信息後，香港郵政會按本條準則第 3.1.7 條所載程序，查清對方確實擁有該私人密碼匙。香港郵政不會擁有申請人之私人密碼匙。
- 查明申請人確實擁有其私人密碼匙後，香港郵政會產生證書，證書內載申請人之公開密碼匙。

b) **代製密碼匙服務**

倘若使用代製密碼匙服務，則由香港郵政代表登記人 生配對密碼匙及製作證書。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。

由以上兩種方式產生之證書會刊登在儲存庫上，登記人可於香港郵政儲存庫 ldap://ldap.hongkongpost.gov.hk 下載。

4.3 發出、核對及接受證書程序

a) 香港郵政擬於申請表所載期限內辦妥申請。香港郵政將對各登記人身分進行認證，倘若且當此等身分得以認證後，通知登記人申請要求之證書已準備就緒有待完成，並發出確保完成證書須遵循之電子互動過程詳細資料。此步驟通常透過向登記人發出一香港郵政電子核證客戶套件來完成，此套件包括唯讀光碟（或替代存儲介質）、個人密碼封套（內載個人辨識密碼）

及使用指示。倘若使用代製密碼匙服務，則由香港郵政代表登記人　生配對密碼匙及製作證書。在此過程中，登記人會有機會檢查證書內容的準確性及真實性。一經確認無誤，系統會　生配對密碼匙並製作證書。以登記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碟或第 3.1.7 條所述替代存儲介質上。軟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安全方式交付予登記人。於　生配對密碼匙的過程中，香港郵政會以恰當的保安控制使其人員無法接觸登記人的私人密碼匙。登記人同意，他們一旦接獲磁片或替代存儲介質，即須完全　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。香港郵政不會製作和保留一份登記人的私人密碼匙副本。

b) 當按照互動程式完成第 4.3(a)條所述證書時，登記人會獲機會核對確定證書中由登記人提供之所有資料及申述均準確無誤。各登記人向香港郵政保證（承諾）其將完成此核對並妥為完成。

(i) 若此證書中有任何不準確或不實之處，登記人必須取消此程序；

(ii) 若（且僅若）證書中無任何不準確或不實之處，登記人可根據所受指示繼續、允許並同意證書完成。透過此等繼續進程，登記人接受根據本準則發出之證書。

(iii) 香港郵政會發出通知要求登記人核實證書內容或下載證書。 如登記人於該通知發出日起三個月內仍未根據指示核實證書內容或下載證書，則登記人協議會自動終止，已繳交的登記費用亦不獲退還。如登記人於上述所指三個月期限屆滿後欲申請電子核證證書，則須向香港郵政重新提交申請及繳交登記費用。

透過接受證書，登記人確認證書中所包含資料正確。接受確認且為登記人同意受本準則、證書申請表及登記人協議條款之約束。

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給登記人的證書（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核證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(h)條）。

不論何時，若有以下情況，香港郵政均可按準則中程序暫停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；或
f) 知道或有理由相信其資料出現在證書上之登記人或獲授權代表：
   i) 死亡或已死亡；
   ii) 在擬撤銷證書前五年內已達成香港法例第六章破產條例所指之債務重整協議或債務償還安排或自願安排；或
   iii) 因欺詐、舞弊或不誠實行為，或違反電子交易條例而在本港或海外被定罪；

若登記人為一機構，而該登記人：
   (i) 正被清盤或接到有司法管轄權之法庭所判清盤令；
   (ii) 在擬撤銷證書前五年內已達成香港法例第六章破產條例所指之債務重整協議或債務償還安排或自願安排；
   (iii) 其董事、職員或僱員因欺詐、舞弊或不誠實行為，或違反電子交易條例被定罪；或
   (iv) 在撤銷證書前五年內登記人資產之任何部分託給接管人或管理人接管。

4.4.2 撤銷程序請求

登記人可透過傳真、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“存留”證書，即可令證書暫時失效。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為止。撤銷證書申請表格可往各郵局索取，或從香港郵政網頁 http://www.hongkongpost.gov..hk下載。香港郵政會考慮登記人的要求，把證書從"存留"的狀態回復為有效。但香港郵政只會在緊慎的情況下處理證書從"存留"的狀態回復為有效。

所有被吊銷或撤銷證書之有關資料（包括表明吊銷及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，查看在 (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，香港郵政決定暫停或撤銷證書，兩個工作日內，暫停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停或撤銷證書後，登記人均不得在交易中使用證書。倘若登記人無視以上規定，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停或撤銷證書(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) 電子核證證書的證書撤銷清單每天更新三次，更新時間為香港時間 09:15、14:15 及 19:00（即格林尼治平時[GMT] 時間 01:15、06:15 及 11:00）。在正常情況下，香港郵政會於更新時間後的十五分鐘內，盡快將最新的證書撤銷清單刊登於網址 "http://www.hongkongpost.gov.hk/crl/eCert.crl" 或 LDAP 儲存庫

"ldap://ldap.hongkongpost.gov.hk"。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刊登時序。香港郵政儲存庫的資料可參閱本準則第 2.5 段。

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

在香港郵政處理撤銷行動並把資料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審核追蹤保安檔案內。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：
    - 處理撤銷及吊銷證書之要求
    - 實際發出、撤銷及吊銷證書
    - 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為七年。

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

4.5.6 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，該收集系統不能為任何應用程式、程序或其他系統程式修改。任何對審核收集系統之修改本身即成為可審核事件。

4.5.7 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

脆弱性評估為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為保存七年。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。

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 存檔備存程序

製作並保存存檔之備存副本，以備初始存檔遺失或損毀。

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

香港郵政電子核證機關、根源密碼匙及證書壽命為期十年。核證機關密碼匙及證書期滿至少三個月前會進行續期。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、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。

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，為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

香港郵政已為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為保存。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。

香港郵政已為所有涉及香港郵政電子核證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為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，否則香港郵政及登記人配對密碼匙之產生程序可使配對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。若由登記人產生其配對密碼匙，則登記人有責任就符合本準則規定之證書而產生其配對密碼匙。倘若由香港郵政　登記人代製密碼匙，私人密碼匙一旦裝入軟碟或 3.1.7 條所述替代存儲介質，系統即將此予以刪除。香港郵政不會製作和保存一份私人密碼匙的副本。

6.1.2 登記人公開密碼匙交付

除了由香港郵政代表登記人按照代製密碼匙的要求　生的配對密碼匙外，登記人之公開密碼匙須以指定方法傳遞予香港郵政，以確保：

- 密碼匙於傳遞過程中未被更改
- 發送人擁有與所傳遞之公開密碼匙相應之私人密碼匙(見第 3.1.7 條)
- 公開密碼匙之發送人為證書申請書中所列人士

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為 2048 位元 RSA。登記人配對密碼匙則為 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

香港郵政電子核證(個人)、(機構)及(伺服器)證書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。電子核證（保密）證書使用之密碼匙只可作加密電子通訊用途（見第 1.2.3(d)條)。

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 1 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核證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 級保安標準的加密硬件裝置加密及儲存。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。所有私人密碼匙不會存檔。

6.3 配對密碼匙管理其他範疇

香港郵政之公開及私人密碼匙使用期不超過十年。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。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

香港郵政控制為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 1 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核證證書之特點摘要。

7.2 證書撤銷清單結構

香港郵政證書撤銷清單之格式為 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為現有證書續期的證書持有人並均具約束力。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。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。各郵政局櫃位均備有本準則之印行本供登記人及倚據證書人士閱覽。

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：

“接受證書”就獲發給某證書者而言，指知悉該證書內容時此人：

a) 批准將該證書向他人公佈或在某儲存庫內公佈；

b) 使用該證書；或

c) 以其他方式表示承認該證書。

“收訊者”就發訊者所發出之任何電子紀錄而言，指發訊者指明接收該紀錄者，但不包括中介人。

“申請人”指申請電子核證之自然人或法人。

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

“獲授權代表”指登記人機構之授權代表。

“授權單位”指登記人機構授權使用簽發予該登記人機構香港郵政電子核證（保密）證書之單位。

“授權用戶”指登記人機構授權使用簽發予該登記人機構香港郵政電子核證（機構）證書之成員或僱員。

“證書”或“電子核證”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) 經發出紀錄核證機關之負責人員簽署。

“核證機關”指向他人(可以為另一核證機關)發出證書者。

“核證作業準則”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、數目字或其他符號為認證或承認該紀錄之目的定立或採用者。

“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為獲發給該證書之人之行為。

“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為認可證書之證書。

“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。

“法律規則”指-

(a) **條例；**

(b) **普通法規則或衡平法規則；或**

(c) **習慣法。**

“安全接層”指使用連接導向、終端對終端加密之互聯網規約，以在客戶（通常為萬維網瀏覽器）與伺服器（通常為網絡伺服器）之間為應用層通訊提供資料保密服務及資料完整性服務，並在客戶與伺服器之間選擇提供等同實體驗證。其 IETF-標準版乃 TLS（傳送層保安）規約，由 RFC2246 指明。

“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。

“登記人”指

(a) **任何人已簽妥登記人協議及**

(i) **在某證書內指名或識別為獲發給證書；**

(ii) **已接受該證書；**

(iii) **持有與列於該證書內的公開密碼匙對應之私人密碼匙；或**

(b) **登記人機構**

“登記人機構” 指獲授權代表已簽署登記人協議及根據此核證作業準則為合資格獲簽發銀行證書(機構)之機構。

“穩當系統”指符合以下所有條件之電腦硬體、軟件及程序：

(a) **合理地安全可免遭受入侵及不當使用；**

(b) **在可供使用情況、可靠性及操作方式能於合理期內維持正確等方面達到合理水平；**

(c) **合理地適合執行其原定功能；及**

(d) **依循廣為接受之安全原則。**

“核實數碼簽署”就某數碼簽署、電子紀錄及公開密碼匙而言，指確定：

(a) **該數碼簽署是否用與列於某證書內之公開密碼匙對應之私人密碼匙產生；及**

(b) **該電子紀錄在數碼簽署產生後是否未經更改，**

而提述數碼簽署屬可核實者，須以此釋義為準。

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

附錄 B - 香港郵政電子核證證書格式

		電子核證（個人）證書	電子核證（個人／未成年人）證書	電子核證（機構）證書
標準欄				
版本		X.509 V3	X.509 V3	X.509 V3
序號		[系統產生]	[系統產生]	[系統產生]
簽署數元		sha1RSA	sha1RSA	sha1RSA
發出人		cn=Hongkong Post e-Cert CA, o=Hongkong Post, c=HK	cn=Hongkong Post e-Cert CA, o=Hongkong Post, c=HK	cn=Hongkong Post e-Cert CA, o=Hongkong Post, c=HK
有效期	不早於	[UTC 時間]	[UTC 時間]	[UTC 時間]
	不遲於	[UTC 時間]	[UTC 時間]	[UTC 時間]
主體名稱		cn=[香港身份證姓名][1], ea=[電子郵箱地址], ou=[登記人參考編號][2], ou=[續期編碼][3] o=Hongkong Post e-Cert (Personal), c=HK	cn=[香港身份證姓名][1], ea=[電子郵箱地址], ou=[登記人參考編號][2], ou=[續期編碼][3] o=Hongkong Post e-Cert (Personal/Minor), c=HK	cn=[姓名], ea= [電子郵箱地址], ou=[登記人參考編號][2], ou=[商業登記編號+註冊證書/登記證書+其他][4], ou=[機構], ou=[機構部門], o=Hongkong Post e-Cert (Organisational), c=HK
登記人公開密碼匙	數元	RSA	RSA	RSA
	公開密碼匙	[在索取證書過程中由登記人瀏覽器中產生及提供；或由香港郵政代製][5]	[在索取證書過程中由登記人瀏覽器中產生及提供；或由香港郵政代製][5]	[在索取證書過程中由登記人產生及提供；或由香港郵政代製][5]
發出人識別名稱		未使用	未使用	未使用
登記人識別名稱		未使用	未使用	未使用
標準延伸欄位[7]				
機關密碼匙識別名稱	發出人	cn=Hongkong Post Root CA, o=Hongkong Post, c=HK	cn=Hongkong Post Root CA, o=Hongkong Post, c=HK	cn=Hongkong Post Root CA, o=Hongkong Post, c=HK
	序號	[從發出人處獲取]	[從發出人處獲取]	[從發出人處獲取]
基本限制	主題	最終實體	最終實體	最終實體
	路徑長度限制	無	無	無
密碼匙的使用		數碼簽署，密碼匙加密	數碼簽署，密碼匙加密	數碼簽署，密碼匙加密
登記人的其他供選擇名稱	DNS 名稱	[經加密的香港身份證號碼][6]	[經加密的香港身份證號碼][6]	未使用
	rfc822	[電子郵箱地址]	[電子郵箱地址]	[電子郵箱地址]
Netscape 延伸欄位[7]				
Netscape 證書類型		SSL client, S/MIME	SSL client, S/MIME	SSL client, S/MIME
Netscape SSL 伺服器名稱		未使用	未使用	未使用
Netscape 備註		香港郵政電子核證證書 有關規管使用此證書之條文條款，請參閱登記人協議及核證作業準則。全港郵政局均備有此兩份文件以供索閱。核證作業準則亦可從 http://www.hongkongpost.gov.hk 網頁瀏覽。	香港郵政電子核證證書 有關規管使用此證書之條文條款，請參閱登記人協議及核證作業準則。全港郵政局均備有此兩份文件以供索閱。核證作業準則亦可從 http://www.hongkongpost.gov.hk 網頁瀏覽。	香港郵政電子核證證書 有關規管使用此證書之條文條款，請參閱登記人協議及核證作業準則。全港郵政局均備有此兩份文件以供索閱。核證作業準則亦可從 http://www.hongkongpost.gov.hk 網頁瀏覽。

附錄 B

香港郵政電子核證證書格式

		電子核證（伺服器）證書	電子核證（保密）證書
標準欄			
版本		X.509 V3	X.509 V3
序號		[系統產生]	[系統產生]
簽署數元		sha1RSA	sha1RSA
發出人		cn=Hongkong Post e-Cert CA, o=Hongkong Post, c=HK	cn=Hongkong Post e-Cert CA, o=Hongkong Post, c=HK
有效期	**不早於**	[UTC 時間]	[UTC 時間]
	不遲於	[UTC 時間]	[UTC 時間]
主體名稱		cn=[URL], ou=[登記人參考編號][2], ou=[商業登記編號+註冊證書/登記證書+其他][4], ou=[機構], ou=[機構部門], o=Hongkong Post e-Cert (Server), c=HK	cn=[單位名稱], ea= [電子郵箱地址], ou=[登記人參考編號][2], ou=[商業登記編號+註冊證書/登記證書+其他][4], ou=[機構], ou=[機構部門], o=Hongkong Post e-Cert (Encipherment), c=HK
登記人公開密碼匙	**數元**	RSA	RSA
	公開密碼匙	[在索取證書過程中由登記人產生及提供]	[在索取證書過程中由登記人產生及提供；或由香港郵政代製][5]
發出人識別名稱		未使用	未使用
登記人識別名稱		未使用	未使用
標準延伸欄位[7]			
機關密碼匙識別名稱	**發出人**	cn=Hongkong Post Root CA, o=Hongkong Post, c=HK	cn=Hongkong Post Root CA, o=Hongkong Post, c=HK
	序號	[從發出人處獲取]	[從發出人處獲取]
基本限制	**主題**	最終實體	最終實體
	路徑長度限制	無	無
密碼匙的使用		密碼匙加密	數碼簽署，密碼匙加密
登記人的其他供選擇名稱	**DNS 名稱**	未使用	未使用
	rfc822	未使用	[電子郵箱地址]
Netscape 延伸欄位[7]			
Netscape 證書類型		SSL server	SSL client, S/MIME
Netscape SSL 伺服器名稱		[URL]	未使用
Netscape 備註		香港郵政電子核證證書 有關規管使用此證書之條文條款，請參閱登記人協議及核證作業準則。全港郵政局均備有此兩份文件以供索閱。核證作業準則亦可從 http://www.hongkongpost.gov.hk 網頁瀏覽。	香港郵政電子核證證書 此類證書只可用作(i) 傳送加密之電子信息予登記人機構；(ii) 容許登記人機構為信息解密；及(iii) 容許登記人機構發出認收信息並附加其數碼簽署以證實其登記人機構收件身分；以及藉此確認已收訖送出之加密信息。有關規管使用此證書之條文條款，請參閱登記人協議及核證作業準則。全港郵政局均備有此兩份文件以供索閱。核證作業準則亦可從 http://www.hongkongpost.gov.hk 網頁瀏覽。

附錄 B

香港郵政電子核證證書格式

附註：

[1] **姓名格式: 英文格式，其中姓氏須要大寫, 例如** CHAN Tai Man David

[2] **登記人參考編號**, 10 **位數字**

[3] **如該證書為已續期證書，則會在此欄位內加上式樣為**":Rxx"**的續期編碼(**xx**為一數值)。如該證書為第一次續期後發出，續期編碼會以**":R01"**表示；如該證書為第二次續期後發出，續期編碼會以**":R02"**表示；如此類推。**

[4] **"商業登記編號"欄位** : 16 **位數字**, **"註冊證書 / 登記證書"欄位** : 8 **位數字**, **"其他"欄位: 最多**30 **位字元 (如有)。香港特別行政區政府部門之"商業登記編號"及"註冊證書 / 登記證書"欄位全部為零("**0"**)，部門簡稱 (例如** HKPO **代表香港郵政) 會放入"其他" 欄位。如該證書為已續期證書，則會在"其他" 欄位內加上式樣為**":Rxx"**的續期編碼(**xx**為一數值)。如該證書為第一次續期後發出，續期編碼會以**":R01"**表示；如該證書為第二次續期後發出，續期編碼會以**":R02"**表示；如此類推。**

[5] 1024-bit

[6] **登記人的香港身份證號碼(包括括號內的數字)(以**hkid_number**表示)將會經登記人私人密碼匙簽署並轉化為一雜湊數值(以**cert_hkid_hash**表示)後，存入證書：**

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

*SHA-1***為一雜湊函數而***RSA***則為簽署函數**

登記人自行產生密碼匙時，hkid_number**會在登記人的瀏覽器中簽署。如屬代製密碼匙，**hkid_number**則會在香港郵政處所內代製密碼時簽署。經簽署的香港身份證號碼 -** $\textbf{\textit{RSA}}_{\textbf{privatekey, sha-1}}$ **(**hkid_number**)會透過保密的通訊渠道傳送往香港郵政核證機關系統。核證機關系統確認登記人的資料後，會產生已簽署的香港身份證號碼的雜湊數值** $\textbf{\textit{SHA-1}}\,(\,\textbf{\textit{RSA}}_{\textbf{privatekey, sha-1}}\,(\,\textbf{hkid\_number}\,)\,)$**。該雜湊數值會輸入證書內的指定延伸欄位。**

[7] **所有標準延伸欄位及**Netscape**延伸欄位均為 "非關鍵" (Non-Critical) 延伸欄位。**

附錄 C - 香港郵政電子核證證書撤銷清單格式 (X.509 第二版)

標準欄位	子欄位	欄位內容	備註
版本		第二版	此欄顯示證書撤銷清單格式的版本
簽署		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		CN=Hongkong Post e-Cert CA 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		[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		[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	用戶證書	[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
	輸入證書撤銷清單資料申延		
	原因代碼 （見附註 2）	[撤銷理由識別碼]	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
標準延伸欄位			
機關密碼匙識別名稱	發出人	CN=Hongkong Post Root CA 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	[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		[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。

附註：

1. 所有標準延伸欄位均為 "非關鍵" (Non-Critical) 延伸欄位。
2. 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」）。

附錄 D - 香港郵政電子核證 – 服務摘要

要點	*電子核證(個人) 證書*	*電子核證(機構) 證書*	*電子核證(伺服器) 證書*	*電子核證(保密) 證書*
認可證書	是	是	是	是
配對密碼匙	1024-bit RSA	1024-bit RSA	最長 1024-bit RSA	1024-bit RSA
香港郵政提供產生密碼匙軟件	是	是	否	是
製造配對密碼匙	由登記人製造或由香港郵政代製	由登記人製造或由香港郵政代製	由登記人製造	由登記人製造或由香港郵政代製
登記人	持有有效之香港身份證者	公司、機構、法定團體、香港特別行政區政府的局、署、處	公司、機構、法定團體、香港特別行政區政府的局、署、處	公司、機構、法定團體、香港特別行政區政府的局、署、處
證書持有人	持有有效之香港身份證者	在香港註冊的機構的成員或僱員	在香港註冊的機構所擁有的互聯網伺服器名稱	在香港註冊的機構的登記單位
核實身份	須當面核實證書持有人的身份	須核實有關機構及獲授權人仕的身份	須核實有關網域名稱、機構及獲授權人仕的身份	須核實有關機構及獲授權人仕的身份
證書的用途	數碼簽署及加密	數碼簽署及加密	SSL 加密	加密
遞交申請	申請人須親身遞交申請	須由獲授權人仕親身遞交申請	須由獲授權人仕親身遞交申請	須由獲授權人仕親身遞交申請
證書上載有登記人身份證號碼的雜湊數值	是	否	否	否
證書上載有獨特的登記人參考號碼	是	是	是	是
證書上載有 (如有) 商業登記證/公司註冊證書號碼	否	是	是	是
載有登記人資料	• 登記人名稱 • 登記人電郵地址	• 登記人名稱 • 登記人電郵地址 • 登記機構名稱	• 登記伺服器名稱 • 登記機構名稱	• 登記單位名稱 • 登記機構名稱 • 登記單位電郵地址
收費 （另見本準則第 2.4 條）	每份證書（包括首次及續期申請）每年 50 港元	每份證書首次申請每年 50 港元，續期申請則為每年 150 港元。每份申請須另繳交行政費 150 港元	每份證書（包括首次及續期申請）每年 2500 港元（包括行政費）	每份證書（包括首次及續期申請）每年 150 港元，每份申請須另繳交行政費 150 港元
證書有效期	一年	一年	一年	一年
倚據限額	50 萬港元	50 萬港元	50 萬港元	25 萬港元