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
「智方便」電子證書

核證作業準則

日期：二零二二年十一月一日
物件識別碼：1.3.6.1.4.1.16030.1.9.2

前言

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

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

設計公匙基建之目的，為支援以上述方式在中華人民共和國香港特別行政區進行商業活動及其他交易。

就條例而言，香港郵政署長為認可核證機關。根據條例，香港郵政署長（其本人或香港郵政署職員）(a)履行核證機關之職能和提供服務，以及與核證機構之職能或服務相關或附帶的服務；及(b)爲任何合宜舉措以履行上述(a)段的目的及與認可核證機關有關的任何條文。

根據政府資訊科技總監頒佈之認可核證機關業務守則第 33 條，香港郵政可以指定代理人或合約分判商，在香港郵政全面管理和監控下進行其若干或所有作業.。

香港郵政根據條例賦予的權力提供核證機關服務，並且由 2007 年 4 月 1 日起，在香港郵政的全面管理和監督下，將核證機關服務外判給承辦商。

香港郵政依然爲條例第 34 條下之認可核證機關，而核證登記機關及承辦商（包括核證登記機關及承辦商之合約分判商）則爲香港郵政根據政府資訊科技總監頒布之認可核證機關業務守則第 3.2 條所委任之代理人，爲香港郵政所委任以履行核證機關之職能。

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、撤銷及利用公開儲存庫公布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。**根據本核證作業準則發出的「智方便」電子證書，均爲條例下的認可證書，在本核證作業準則內稱爲“證書”或“「智方便」電子證書”。**

本核證作業準則列載「智方便」電子證書之實務守則，其結構如下：

第 1 條載有概述及聯絡資料
第 2 條列載各方職能及義務
第 3 條列載身分辨識與驗證要求
第 4 條概述運作要求
第 5 條介紹保安監控措施
第 6 條列載如何產生及控制公開/私人配對密碼匙
第 7 條概述證書、證書撤銷清單及線上證書狀態應答資料

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，並規定香港郵政在發出證書時採用之實務守則。

香港郵政已獲 Internet Assigned Numbers Authority (IANA) 分配私人企業號碼 (Private Enterprise Number) 16030 號。就識別準則之言，“1.3.6.1.4.1.16030.1.9.2”爲本準則的物件識別碼(Object Identifier, OID)（見**附錄** B 內關於證書政策(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、撤銷及公布的「智方便」電子證書）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。

為香港居民提供免費的數碼個人身分，是 2017 年 10 月公布的數碼基礎設施項目之一。政府已經展開相關的數碼基礎設施並命名為「智方便」平台。「智方便」為所有香港居民提供數碼個人身分，使他們能夠以單一的數碼身分和認證與政府和商業進行網上交易。

香港居民可以透過各個提供各種「智方便」版本的登記渠道獲取「智方便」。只有按照本準則第 3.1.1 條在「智方便」核證登記地點登記的「智方便」持有人，方有資格申請「智方便」電子證書。

香港郵政根據本準則所簽發的「智方便」電子證書，是特別指明為已在「智方便」核證登記地點登記的「智方便」持有人，根據條例提供具法律效力的數碼簽署。除特別聲明外，本作業準則各章節中提到的「智方便」版本是指根據本準則第 3.1.1 條在「智方便」核證登記地點獲取的「智方便」版本，在本準則內稱為「智方便」。

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「智方便」電子證書，香港郵政已指明爲認可證書。根據條例，「智方便」電子證書享有認可證書的地位，其用於數碼簽署的交易受到條例的認可和保護。

「智方便」電子證書支援公匙基建模式，即登記人可以遠程接達儲存在「智方便」系統所托管的硬體安全模組中的私人密碼匙，且登記人的「智方便」電子證書配對密碼匙在硬體安全模組中製作並儲存。

附錄 D 載有「智方便」電子證書特點摘要。

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。香港郵政乃唯一被授權根據本準則發出「智方便」電子證書之核證機關（見第 2.1.1 條）。

1.2.1.1 生效

香港郵政於儲存庫公布「智方便」電子證書。

1.2.1.2 香港郵政進行合約分判之權利
香港郵政可指定代理人或合約分判商履行本準則及登記人協議規定之部份或全部職能。無論是否有任何指定，香港郵政仍爲認可核證機關及會履行「智方便」電子證書發出人的職能。

1.2.2「智方便」核證登記辦事處
香港郵政通常透過「智方便」核證登記辦事處處理「智方便」電子證書申請人或登記人之事宜。政府資訊科技總監辦公室履行「智方便」核證登記辦事處的職能，或指定承辦商履行部份或全部「智方便」核證登記辦事處的職能。「智方便」核證登記辦事處是代表香港郵政的核證登記機關執行以下職責：

a) 接受和處理申請人及登記人的證書申請；
b) 核實申請人及登記人之身分；
c) 保留核實申請人和登記人身分證明文件的文本；及
d) 通知申請人及登記人有關已批准或被拒絕的證書申請，及已撤銷的證書。

下文第 2.1.2 條載有「智方便」核證登記辦事處需履行的所有職能。

1.2.3 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。

倚據證書人士需注意：十八歲以下的人士亦可按本準則第 3 條及第 4 條，申請「智方便」電子證書。

1.2.3.1 私人密碼匙的位置
「智方便」電子證書之私人密碼匙將儲存於「智方便」系統所托管的硬體安全模組。香港郵政將於儲存庫公布「智方便」電子證書（連同公開密碼匙），供公眾下載及核對數碼簽署。

1.2.3.2 登記人及「智方便」核證登記辦事處
登記人必須授權「智方便」核證登記辦事處保管和管理私人密碼匙，並保存一份由香港郵政發給登記人的「智方便」電子證書。登記人確認「智方便」核證登記辦事處亦可同時代表香港郵政履行以上第 1.2.2 條所述的職能。登記人確認並同意「智方便」核證登記辦事處的有關職能不會造成利益衝突，「智方便」核證登記辦事處擔任的職能亦同時對所有人士有利。

1.2.4 證書之類別
「智方便」電子證書是唯一根據本準則由香港郵政發出的證書類別。香港郵政僅簽發「智方便」電子證書予已以適當形式確定接受登記人協議，且其身分及其證書申請已根據本準則第 3 條和第 4 條被「智方便」核證登記辦事處成功核實及接受之申請人士。登記人可以透過「智方便」系統，與接受「智方便」電子證書數碼簽署的倚據證書人士進行政府及商業交易。

「智方便」電子證書可發出予十八歲以下的人士（另見第 3.1.3 條）

1.2.5 證書之期限
根據本準則「智方便」電子證書的有效期由發出自香港郵政當日起即日生效，有效期為一年。

1.2.6 申請
所有「智方便」電子證書的首次申請及續期申請，申請人須符合本準則第 3 及 4 條所述的要求。

1.2.7 適用性
發出予登記人的「智方便」電子證書可用於一般用途，並沒有受限制用於特定類型之交易。

1.3 聯絡資料

申請人或登記人可經由以下途徑就「智方便」電子證書作出查詢、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：29216633
傳真：27759130
電郵地址：enquiry@eCert.gov.hk

1.4 處理投訴程序

香港郵政會儘快處理所有以書面及口頭作出的投訴，並在收到投訴後十個工作日內給予詳細的答覆。若十個工作日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儘快以電話、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 職能和義務

香港郵政之職能乃由本準則以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。

2.1.1 核證機關之職能和義務

根據本準則，香港郵政履行以下之職能（「智方便」核證登記辦事處或承辦商在香港郵政的管理和控制下可以履行以下任何或所有職能）：

a) 透過「智方便」核證登記辦事處接受「智方便」電子證書申請；
b) 透過「智方便」核證登記辦事處通知申請人有關已批准或被拒絕的申請；
c) 根據「智方便」核證登記辦事處遞交的簽發證書要求，發出「智方便」電子證書，並於儲存庫公布「智方便」電子證書；
d) 撤銷「智方便」電子證書並依時公布修訂的證書撤銷清單；
e) 提供用於檢查「智方便」電子證書狀態之線上證書狀態應答（“OCSP”）；
f) 透過「智方便」核證登記辦事處通知登記人有關已撤銷的「智方便」電子證書。

根據條例，香港郵政負責使用穩當系統履行其服務以（a）發出或撤銷「智方便」電子證書；或（b）利用儲存庫公布已發出之「智方便」電子證書，或給予通知書與已撤銷之「智方便」電子證書。

2.1.2「智方便」核證登記辦事處之職能及義務

「智方便」核證登記辦事處履行以下之職能（承辦商在「智方便」核證登記辦事處的管理和控制下可以履行以下任何或所有職能）：

<u>代表香港郵政履行核證登記機關之職能（見第 1.2.2 條）</u>

a) 接受和處理申請人之證書申請，申請人必須為「智方便」持有人（見第 3.1.1 條）；
b) 在首次申請或續期申請「智方便」電子證書時核實申請人/登記人之身分（見第 3.1.2 條及第 3.2.1 條），並在「智方便」系統中為身分核實結果作紀錄；
c) 為任何撤銷「智方便」電子證書的要求核實登記人的身分；
d) 根據本準則條款及登記人協議，在整個證書有效期內及相關證書到期後至少 7 年內，保存所有用作核實申請人為「智方便」持有人身分的記錄。
e) 當收到香港郵政通知後，通知申請人/登記人有關證書申請及撤銷證書要求已獲批准或被拒絕的結果；
f) 告知登記人其義務，包括有責任維護用於透過「智方便」系統接達「智方便」電子證書的「智方便」憑證，以及即時透過「智方便」系統或其他由「智方便」核證登記辦事處指定之通訊渠道向「智方便」核證登記辦事處呈報任何外洩或懷疑外洩的事件；

<u>其他職能</u>

g) 在申請人確認接受登記人協議條款及條件後，向香港郵政遞交證書申請要求；
h) 為登記人製作配對密碼匙，並將其私人密碼匙儲存在「智方便」系統的硬體安全模組內；
i) 保管和管理登記人的私人密碼匙，並確保只有登記人才可使用其私人密碼匙進行數碼簽署；

j) 當「智方便」電子證書在儲存庫、證書撤銷清單或線上證書狀態應答中顯示證書狀態為已過期或已撤銷狀況時，確保登記人或任何其他人士不能再使用該「智方便」電子證書的私人密碼匙；
k) 產生並遞交簽發證書要求給香港郵政，其中包括了與申請人有關的資料以及確認同意接受登記人協議的條款及條件。

「智方便」核證登記辦事處負責使用穩當系統交付上述職能。

香港郵政依然對「智方便」核證登記辦事處在其執行或聲稱執行上述涉及核證機關之義務和職責的行為負責。「智方便」核證登記辦事處僅代表香港郵政執行香港郵政在核證登記機關功能中的義務和職責。

2.1.3 承辦商之職能及義務

承辦商僅根據其與香港郵政之間之合約之規定向香港郵政承擔責任。根據該等合約，香港郵政任命承辦商爲其代理人營運並維持系統以簽發「智方便」電子證書。此外，在香港郵政的全面管理和控制下，香港郵政可以不時任命該承辦商或其他任何代理人或承辦商，執行所有或任何陳述於本準則之職能。

2.1.4 申請人及登記人之義務

2.1.4.1 申請人之義務

在不影響申請人於本準則和登記人協議規定的其他義務的前提下，申請人對以下所有事項負責：

a) 通過「智方便」系統適當地完成申請程序，並確保在申請證書時作出準確的陳述和保證；
b) 以香港郵政指明的形式確認接受登記人協議，並履行該登記人協議規定其承擔之義務；
c) 同意「智方便」系統在收到申請人的「智方便」電子證書申請後，產生簽發證書要求並發給香港郵政，其要求包括了申請人相關資料及申請人確認接受登記人協議條款及條件；
d) 確認「智方便」電子證書申請一旦遞交，申請人同意「智方便」系統收訖「智方便」電子證書即被視為申請人接受「智方便」電子證書，並授權香港郵政向其他人士或於香港郵政儲存庫內公布其「智方便」電子證書。

2.1.4.2 登記人之義務

在不影響登記人於本準則和登記人協議規定的其他義務的前提下，登記人對以下所有事項負責：

a) 同意「智方便」核證登記辦事處透過「智方便」系統產生登記人之配對密碼匙並儲存其私人密碼匙於「智方便」核證登記辦事處處所內的環境下及硬體安全模組內；
b) 按照本準則所載之規定辦理證書首次申請與證書續期；
c) 不時將由登記人提供之證書資料之任何變動通知「智方便」核證登記辦事處；
d) 如發生可能致使香港郵政有權根據下文第 4 .2 條所載之理由撤銷證書的任何事件，立即通知「智方便」核證登記辦事處；
e) 同意證書一經發出，即向香港郵政以及所有倚據證書人士保證及表明，在證書之有效期間，本準則第 9.6.2 條載明之保證及陳述乃屬並將保持真實、準確及完整；
f) 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，或根據第 4.2 條所述登記人已作出撤銷申請或已從香港郵政收到撤銷通知書的情況下，均不得在交易中使用證書；
g) 在明知香港郵政可能據以撤銷證書之任何事項之情況下，或根據第 4.2 條所述登記人已作出撤

銷申請或已香港郵政收到撤銷通知書的情況下，須立即通知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被撤銷（由香港郵政或登記人本人要求），並明確說明，在此情形下倚據證書人士不得就交易而倚據該證書。

2.1.5 倚據證書人士之義務

在不影響倚據證書人士於本準則和登記人協議規定的其他義務的前提下，倚據「智方便」電子證書之倚據證書人士對以下所有事項負責：

a) 倚據證書人士於倚據「智方便」電子證書時如考慮過所有因素後確信倚據證書實屬合理，方可倚據該等證書；
b) 於倚據該「智方便」電子證書前，確定「智方便」電子證書及其支援的任何數碼簽署用於適當的用途；
c) 履行第 9.6.3 條中列載之所有行爲。

2.2 收費

「智方便」電子證書免費提供給登記人。

2.3 公布資料及儲存庫

根據條例之規定，香港郵政維持一儲存庫，內有根據本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「智方便」電子證書有關之其他資料。除平均每周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、每周 7 日開放。香港郵政會把經由登記人接受並按本準則發出的「智方便」電子證書，儘快在儲存庫作出公布。香港郵政儲存庫可通過下述 URL 接達：

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

2.3.1 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。

2.3.2 證書儲存庫進入要求

經授權之香港郵政人士方可進入儲存庫更新及修改內容。

2.3.3 證書儲存庫更新

儲存庫會於「智方便」系統收到香港郵政發出「智方便」電子證書或香港郵政透過「智方便」核證登記辦事處收到申請人的證書撤銷清單更新要求時盡快作出更新。

2.3.4 核準使用證書儲存庫內的資料

證書儲存庫內的資料，包括個人資料，會按照條例之規定且在符合方便進行合法電子交易或通訊之目的下作出公布。

2.4 遵守規定之評估

須根據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，檢視香港郵政發出、撤銷及公布「智方便」電子證書之系統是否妥善遵守本準則。

3. 身分辨識與驗證要求

3.1 首次申請

3.1.1「智方便」持有人為先決條件

香港居民可利用不同的註冊渠道獲取「智方便」，只有在「智方便」核證登記地點登記的「智方便」持有人，方有資格申請「智方便」電子證書。

香港居民在提供香港身份證及其本人成功通過「智方便」核證登記辦事處的身分核實後，即可在「智方便」核證登記地點獲得「智方便」。他們可到「智方便」核證登記地點，透過配備讀卡器的特定裝置進行登記，該讀卡器可識別香港身份證的真偽，並讀取儲存在香港身份證晶片內的身分資料（包括英文姓名、中文姓名（如有）、香港身份證號碼、簽發日期、出生日期及性別）。如該特定裝置不配備讀卡器，處於「智方便」核證登記地點的人員會核實登記者香港身份證的真偽並輸入登記者的身分資料到「智方便」系統。登記者於「智方便」核證登記地點提供的身分資料及現場拍攝的照片將會傳遞到入境事務處的支援電腦系統，用作核對其與入境事務處的記錄是否相符，以確認登記者是否香港居民，其提供的身分資料是否真確，及其現場拍攝的照片與入境事務處的記錄是否吻合。如沒有於現場拍攝照片，「智方便」核證登記地點的人員會面對面檢查登記者的身份證並認證登記者之容貌是否與載於香港身份證上的照片相符。

3.1.2 初次申請

「智方便」電子證書的申請人必須透過「智方便」系統遞交證書申請。「智方便」電子證書的申請人必須為「智方便」持有人（請參閱第 3.1.1 條）。「智方便」核證登記辦事處及其承辦商將核實申請人「智方便」持有人的身分（i）透過「智方便」系統雙重認證程序，或（ii）申請人在「智方便」核證登記地點進行登記，且其身分獲得核實並成功登記「智方便」（請參閱第 3.1.1 條）。當身分核實完成後，「智方便」核證登記辦事處會將證書申請遞交給香港郵政。

香港郵政會透過「智方便」系統向成功遞交證書申請的申請人發出「智方便」電子證書。申請人同意「智方便」系統收訖「智方便」電子證書即被視為申請人接受「智方便」電子證書。

3.1.3「智方便」電子證書上列出的登記人名稱

透過證書上的主體名稱，包括依據第 4.1 條中的程序所核實的登記人姓名，可識別「智方便」電子證書登記人之身分。登記人香港身份證號碼會以雜湊數值形式儲存於證書內（見**附錄 B**）。

就發出予十八歲以下人士的「智方便」電子證書而言，透過上文提及之證書上的主體名稱及 “iAM Smart-Cert (Minor)”字樣（見**附錄 B**），可識別登記人之身分，及顯示登記人獲發出「智方便」電子證書時未滿 十八歲。

3.1.4 證明有權使用私人密碼匙之方法

「智方便」核證登記辦事處通過使用登記人的私人密碼匙產生數碼簽署。登記人的私人密碼匙儲存在「智方便」系統的硬體安全模組內。登記人在使用私人密碼匙來產生數碼簽署前，必須根據「智方便」核證登記辦事處的規定，通過嚴格的驗證程序（即雙重認證程序）以核實登記人其「智方便」持有人的身分。

「智方便」核證登記辦事處之獲授權人員必須通過由「智方便」核證登記辦事處設計之嚴格的驗證程序後，方可配置、操作和維護儲存了由「智方便」核證登記辦事處保管之私人密碼匙之「智方便」系統。

3.2 證書續期

3.2.1「智方便」電子證書續期

「智方便」核證登記辦事處將在證書有效期屆滿前至少一個月通知登記人續期。 證書續期程序如下：

（a）「智方便」核證登記辦事處透過電子方式向登記人發出續期通知；
（b）登記人同意授權「智方便」核證登記辦事處為「智方便」電子證書續期，並透過「智方便」系統的雙重認證程序核實其「智方便」持有人的身分；
（c）登記人透過「智方便」系統向香港郵政遞交續期申請。

香港郵政不會為已過期或被撤銷的證書續期。

3.2.2 已過期或已撤銷的「智方便」電子證書

香港郵政會在儲存庫中發布所有已過期和被撤銷證書的資料，並注明其過期或被撤銷的狀態。此外，已被撤銷的證書也會在證書撤銷清單內發布。

下文第 4.2.3（a）條規定了用於顯示證書被撤銷狀態的證書撤銷清單的更新時間。至於更新儲存庫以顯示過期「智方便」電子證書狀態的時間，香港郵政將在證書到期後在儲存庫內更新過期狀態。香港郵政還會提供線上證書狀態應答，以檢查「智方便」電子證書的撤銷狀態。

在允許登記人使用「智方便」電子證書之前，「智方便」核證登記辦事處將檢查登記人的「智方便」電子證書的有效期以核實「智方便」電子證書是否已過期，並透過檢查線上證書狀態應答，或者在沒有在線上證書狀態的情況下檢查證書撤銷清單，以核實「智方便」電子證書是否被撤銷。「智方便」核證登記辦事處有責任進行上述核實，以確保「智方便」電子證書在已過期或被撤銷的情況下，其登記人或任何其他人都無法再使用該「智方便」電子證書。

3.2.3 定期審核

「智方便」系統至少每月一次審核登記人其「智方便」的有效性，當中包括審核登記人之：

（a）死亡記錄；
（b）香港居民身分；
（c）香港身份證上顯示的個人資料（包括英文姓名，中文姓名（如有），香港身份證號碼，出生日期和性別）；和
（d）「智方便」持有人的身分。

如果定期審核顯示某登記人的「智方便」因登記人死亡或失去其香港居民身分或根據本準則第 3.2.3（c）條更改了其個人資料而失效，則「智方便」核證登記辦事處將吊銷登記人的「智方便」，並在符合《個人資料（私隱）條例》（第 486 章）第 30（5）條的通報要求後，通知香港郵政撤銷登記人的「智方便」電子證書。 當香港郵政撤銷登記人的「智方便」電子證書後，「智方便」核證登記辦事處將立即通知登記人。

如果定期審核顯示根據本準則第 3.2.3（d）條登記人不再是「智方便」的持有人，則「智方便」核證登記辦事處將通知香港郵政撤銷「智方便」電子證書，並在證書撤銷後立即通知登記人。

如果「智方便」電子證書已被撤銷，符合資格的登記人仍可申請新的「智方便」電子證書。

4. 運作要求

除特別聲明外，此 4.1 條所有規定適用於「智方便」電子證書的申請和發出。

4.1 證書申請、發出和公布

4.1.1 證書申請

4.1.1.1
首次申請「智方便」電子證書的申請人必須為「智方便」持有人（請參閱第3.1.1條），並且必須透過「智方便」系統遞交證書申請要求和接受登記人協議條款及條件。

4.1.1.2
香港居民只有在「智方便」核證登記辦事處核實其身分資料（包括英文姓名、中文姓名（如有）、香港身份證號碼及簽發日期、出生日期、性別和香港居民身分）後，才會被獲發「智方便」（請參閱第 3.1.1 條）。「智方便」電子證書申請人必須為「智方便」持有人（請參閱第 3.1.1 條）。「智方便」核證登記辦事處代表香港郵政核實以確保申請人為「智方便」持有人的身分（i）透過「智方便」系統雙重認證程序或（ii）申請人在「智方便」核證登記地點進行登記，且其身分獲得核實並成功登記「智方便」（請參閱第 3.1.1 條）。在不影響條例第 40 條所述之前提下，香港郵政確認有關該等資料，其將不會進行任何進一步的核實，香港郵政將根據其現有之狀態（即“申請人為「智方便」持有人，並且申請人的身分資料已獲「智方便」核證登記辦事處核實” ）接受該等資料。

4.1.2 發出證書

4.1.2.1
若成功核實申請人「智方便」持有人之身分，「智方便」核證登記辦事處會在其處所內的環境下使用「智方便」系統內的硬體安全模組（HSM）產生申請人之私人密碼匙和公開密碼匙。「智方便」核證登記辦事處負責確保私人密碼匙不會被篡改。

4.1.2.2
「智方便」核證登記辦事處會在其處所內一套可靠的系統及環境下產生包含公開密碼匙的「簽發證書要求」（CSR）。「智方便」核證登記辦事處將準備一個包含申請人資料、申請人接受登記人協議記錄和簽發證書要求的界面檔案。界面檔案將以電子形式遞交給香港郵政。

4.1.2.3
一旦從「智方便」核證登記辦事處收到簽發證書要求，香港郵政會通過使用內含的公開密碼匙檢查證書署名請求架構上的數碼簽署來核實「智方便」核證登記辦事處持有相應的私人密碼匙。香港郵政不會擁有申請人的私人密碼匙。

4.1.2.4
一旦核實「智方便」核證登記辦事處持有相應的私人密碼匙，香港郵政會產生包含申請人公開密碼匙的「智方便」電子證書，並會以安全的方式將發出的「智方便」電子證書傳送到「智方便」核證登記辦事處。

4.1.2.5
「智方便」核證登記辦事處會連接申請人的「智方便」至「智方便」電子證書，以啟動申請人之電子證書，並透過「智方便」系統來通知申請人其「智方便」電子證書申請已完成。

4.1.2.6
申請人透過「智方便」系統遞交「智方便」電子證書申請，當「智方便」系統收訖其「智方便」電子證書時，即表示申請人接受「智方便」電子證書。一旦申請人成功申請和接受「智方便」電子證書，其已發出的「智方便」電子證書會根據條例第 36條於香港郵政儲存庫內公布。

4.1.2.7
「智方便」核證登記辦事處一旦收訖申請人的「智方便」電子證書，會保管其私人密碼匙。

4.1.2.8
所有於「智方便」核證登記辦事處和香港郵政之間以電子形式傳輸的資料必須採用雙方同意的規約進行。

4.1.3 公布證書
香港郵政會盡快在儲存庫公布已發出並獲接受的「智方便」電子證書。申請人可透過儲存庫核實證書上的資料。

4.2 撤銷證書

4.2.1 撤銷證書的情況

4.2.1.1
若核證機關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。在核證機關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（請參閱第 4.6.2 條）。

4.2.1.2
若登記人之登入「智方便」的憑證已經或者被懷疑已經外洩，登記人必須立刻遵照本準則中規定的撤銷程序向香港郵政（透過「智方便」核證登記辦事處）申請撤銷證書。

4.2.1.3
若私人密碼匙或保存公開密碼匙相對應之私人密碼匙之硬體安全模組已經或者被懷疑已經外洩，「智方便」核證登記辦事處必須立即通知香港郵政並向香港郵政申請撤銷「智方便」電子證書。「智方便」核證登記辦事處必須立即通知相關「智方便」電子證書的登記人，上述有關通知香港郵政和向香港郵政申請撤銷已發給該等登記人之「智方便」電子證書。

4.2.1.4
一旦發生任何以下有關「智方便」電子證書的情況或懷疑有該等情況發生，香港郵政將立即撤銷該等「智方便」電子證書，更新證書撤銷清單（CRL）並透過線上證書狀態應答回應其撤銷狀態，屆時香港郵政將透過「智方便」核證登記辦事處通知登記人（「撤銷證書通知書」）：

a) 「智方便」電子證書之私人密碼匙已外洩；
b) 「智方便」電子證書之細節不真實或已變得不真實或證書不可靠；

c) 「智方便」電子證書並非根據本準則妥當發出；
d) 獲得發出「智方便」電子證書之登記人未履行本準則或登記人協議列明之責任；
e) 證書適用之規則或法例有此規定；
f) 獲得發出「智方便」電子證書之登記人死亡或喪失香港居民身分或已更改顯示於其香港身份證上的個人資料（請參閱第3.2.3(a)-(c)條），導致登記人之「智方便」失效；
g) 登記人停止作為「智方便」的持有人（請參閱第3.2.3(d)條）
h) 「智方便」電子證書（未成年人士）之登記人年滿18歲。

4.2.1.5
當香港郵政根據第 4.2.1.4 條發出撤銷通知書予「智方便」電子證書之登記人，「智方便」核證登記辦事處必須立即停止使用該「智方便」電子證書，並且不得允許「智方便」電子證書之相關的私人密碼匙被使用。

4.2.2 撤銷程序請求

4.2.2.1
登記人可透過「智方便」核證登記辦事處的「智方便」系統或其他「智方便」核證登記辦事處指定的溝通渠道向香港郵政提出撤銷證書之申請。登記人不得直接向香港郵政提交申請。

4.2.2.2
當登記人發出撤銷證書請求，「智方便」核證登記辦事處將代表香港郵政就登記人進行身分核實。當登記人身分核實完成後，「智方便」核證登記辦事處將立即把撤銷請求轉交予香港郵政。

4.2.2.3
當香港郵政收到「智方便」核證登記辦事處之撤銷請求後，香港郵政將立即撤銷該證書。

4.2.2.4
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（請參閱第 7.2 條），並可以透過線上證書狀態應答來檢查（請參閱第 7.3 條）。

4.2.3 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) 香港郵政根據第 4.2.2 條規定，透過「智方便」核證登記辦事處從登記人處確切收到撤銷證書之請求後，或(2)香港郵政根據第 4.2.1.4.條規定發出撤銷證書通知書後，將證書該撤之狀態於證書撤銷清單公布。然而，證書撤銷清單並不會於各證書撤銷後隨即在公眾目錄中公布，而只會在下一份證書撤銷清單更新並公布時，才會反映該證書已撤銷之狀態。如附錄 C 第 2 段所述，證書撤銷清單每日於香港時間 0915, 1415 和 1900 公布，並存檔至少七年。

香港郵政會以合理的方式，根據第 4.2.1.4.條規定，透過「智方便」核證登記辦事處發出撤銷證書通知予有關登記人。

b) 在以下任何情況發生之後，登記人均不得使用其姓名登記之證書：
(i) 登記人獲悉香港郵政根據本準則中的條款（包括第 4.2.1.4 條規定的事項）可能據以撤銷證書之任何情況；或

(ii) 登記人根據第 4.2.2.1.條規定透過「智方便」核證登記辦事處向香港郵政提出撤銷證書請求。

倘若登記人在以上任何情況發生之後，仍在任何交易中使用該等證書，則香港郵政和「智方便」核證登記辦事處無須就任何該等交易向登記人或倚據證書人士承擔任何責任。

c) 此外，一旦發生上述 b 項（i）至（ii）中列載的任何有關情況，登記人須立即通知倚據證書人士，告知其不得在交易中倚據登記人之證書。無論登記人是否已通知倚據證書人士不得在交易中倚據登記人之證書，香港郵政和「智方便」核證登記辦事處無須就該等交易向登記人和倚據證書人士承擔任何責任。

對於從香港郵政由做出撤銷證書之決定（不論是應要求或是自行作出該等決定）至該等證書撤銷出現在證書撤銷清單上之間的期間內或至線上證書狀態應答更新了回應證書撤銷狀態之間的期間內所發生的交易，以及在此之後使用任何已撤銷證書所引起之任何交易，香港郵政和「智方便」核證登記辦事處無須就該等交易向登記人和倚據證書人士承擔任何責任。

d) 證書撤銷清單、香港郵政授權撤銷清單（ARL）會依據在**附錄 C** 內指明的時間表及格式更新及公布。

4.2.4 撤銷之生效時間

在不影響上述第 4.2.3 條 b 至 d 項的前提下，在撤銷狀態出現在證書撤銷清單上，或在線上證書狀態應答更新了撤銷狀態之時，該證書即告終止。儘管有上述關於終止證書之生效時間（或在其之後）之規定，對違反第 4.3.3 條 b 項或其他可適用之規定而使用證書的行爲，香港郵政和「智方便」核證登記辦事處概不負責。倚據證書人士在倚據「智方便」電子證書進行交易前，必須查核儲存庫、證書撤銷清單和/或相關之線上證書狀態應答。然而，如果「智方便」核證登記辦事處已妥當地履行了第 3.2.2 條列載的義務，已過期或已撤銷之「智方便」電子證書均不可能再被授權使用（如適用）。

4.3 電腦保安審核程序

4.3.1 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踪保安檔案內。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：
  - 處理撤銷證書之要求
  - 實際發出及撤銷證書
  - 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
- 產生及簽署線上證書狀態應答
- 核證機關密碼匙轉換
- 檔案備存
- 密碼匙緊急復原

4.3.2 處理紀錄之次數
香港郵政每日均會處理及覆檢審核運行記錄，用以審核追踪有關香港郵政的行動、交易及程序。

4.3.3 審核記錄之存留期間
存檔審核記錄文檔存留期爲至少七年。

4.3.4 審核記錄之保護
香港郵政處理審核記錄時實施多人式控制，可提供足夠保護，避免有關記錄意外受損或被人蓄意修改。

4.3.5 審核記錄備存程序
香港郵政每日均會按照預先界定程序（包括多人式控制）爲審核記錄作適當備存。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。

4.3.6 審核資料收集系統
香港郵政系統審核記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。

4.3.7 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。

4.3.8 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。

4.4 記錄存檔

4.4.1 存檔記錄類型
香港郵政須確保存檔記錄記下足夠資料，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，以及所有線上證書狀態應答
f) 定期事件記錄
g) 其他需要以核實存檔內容之數據，以及
h) 證書申請的相關文件，證書批准或拒絕的資料以及登記人協議。

4.4.2 存檔保存期限
密碼匙及證書資料須妥爲保存最少七年。審核跟踪文檔須以香港郵政視爲適當之方式存放於系統內。

4.4.3 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，可避免未經授權之進入。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。

4.4.4 存檔備存程序
在有需要時製作並保存存檔之副本。

4.4.5 電子郵戳
存檔資料均注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。

4.5 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「智方便」電子證書的香港郵政核證機關根源證書，在**附錄 E** 列載其有效期由產生之時起計算不超過二十五年。香港郵政核證機關根源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，相連之根源證書會在香港郵政網頁 http://www.eCert.gov.hk 公布，供大眾取用。原先之根源密碼匙則保留至第 4.4.2 條指定之最短之時限，以供核實用原先之根源密碼匙產生的任何簽署。

4.6 災難復原及密碼匙資料外洩之應變計劃

4.6.1 災難複原計劃
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保證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的地點。業務持續運作計劃每年均會檢討及進行演練。

如發生嚴重故障或災難，香港郵政即時知會政府資訊科技總監，並公布將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。

在發生災難後但穩妥可靠的環境尚未重新確立前的這一期間內，香港郵政將無法更新證書撤銷清

單，也無法返回線上線上證書狀態應答。登記人可以繼續使用「智方便」電子證書，但須自負風險。香港郵政亦無法發出證書，撤銷證書或開放儲存庫供下載公共密碼匙和證書。

4.6.2 密碼匙資料外洩之應變計劃

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「智方便」電子證書的核證機關私人密碼匙資料外洩，香港郵政會即時知會政府資訊科技總監並作出公布。核證機關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。

4.6.3 密碼匙的替補

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的「智方便」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政府資訊科技總監並作出公布。公布內容包括已撤銷證書的名單、如何爲登記人提供新的核證機關公開密碼匙及如何向登記人重新發出證書。

4.7 核證機關終止服務

如香港郵政停止擔任認可核證機關之職能，即按“香港郵政終止服務計劃”所定程序知會政府資訊科技總監並作出公布。在終止服務後，香港郵政會將核證機關的紀錄適當地存檔至少七年（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。

根據香港郵政終止服務計劃，香港郵政會在終止服務生效前至少九十天知會政府資訊科技總監其準備終止「智方便」電子證書有關服務。香港郵政會在終止服務生效前至少六十日，透過電子郵件、信件或者透過「智方便」系統通知所有登記人其準備終止作爲認可核證機關之服務。香港郵政認可核證機關將會在香港發行的一家英文日報（如可行）以及一家中文日報上刊載其準備終止作爲認可核證機關之服務。該等公告必須在終止服務生效前至少六十日刊發，且必須持續刊載三天。

4.8 「智方便」核證登記辦事處終止服務

無論是什麼原因的情況下，若「智方便」核證登記辦事處停止擔任根據本準則之核證登記機關，經「智方便」核證登記辦事處發出的「智方便」電子證書也將同時被撤銷。香港郵政和「智方便」核證登記辦事處無須對任何人因證書撤銷所引起的索賠、法律程序、債務、損失（包含任何直接或間接的損失、任何收益損失、利潤、商業機會、合約或預期存款）、損害（包含任何直接、特殊、間接或從屬的任何性質的損害）或任何損失或費用承擔任何責任。

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。

5.1.2 進入控制
香港郵政實施商業上具備合理之實體保安控制措施，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），而可使用該等硬體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。

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 防火及消防保護
核證機關設施備妥防火計劃及滅火系統。

5.1.6 媒體存儲
媒體存儲及處理程序已經開發備妥。

5.1.7 場外備存
香港郵政核證機關系統數據之適當備存會另行儲存於其他場所，並獲足夠保護，以免被盜用、損毀及媒體衰變。(另見第 4.6.1 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受限制之運作）之香港郵政、「智方便」核證登記辦事處或承辦商之僱員、合約分判商以及顧問（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「智方便」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。香港郵政進行按角色及責任訂定各級實體及系統接達控制，以及採取職責分離措施，以維護有關程序之完整性。

5.2.2 香港郵政、承辦商與「智方便」核證登記辦事處之間的文件及資料傳遞
香港郵政、「智方便」核證登記辦事處與承辦商之間的所有文件及資料的傳遞，均使用香港郵政規定且獲得「智方便」核證登記辦事處和承辦商同意之協約，以慣常的控制及安全方式進行。

5.2.3 年度評估
評估工作每年執行一次，以確保符合政策及工作程序控制之規定（見第 2.4 條）。

5.3 人員控制

5.3.1 背景及資格
香港郵政、「智方便」核證登記辦事處及承辦商採用之人員及管理政策，可合理確保各自之人員（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
根據本準則之規定，香港郵政會調查及 /或要求「智方便」核證登記辦事處和承辦商調查擔任受信職責之人員（在其受聘/加入前及其後有需要時定期進行），以核實該等人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、「智方便」核證登記辦事處人員與承辦商人員均已接受了履行其職責所需要之初步培訓。有需要時，香港郵政、「智方便」核證登記辦事處與承辦商亦會提供持續培訓，使其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、「智方便」核證登記辦事處人員及承辦商人員會收到綜合用戶手冊，其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由多人式控制之可防止篡改硬件裝置內進行。

6.1 產生及安裝配對密碼匙

6.1.1 產生配對密碼匙
除非程序被獲授權使用者外洩，否則香港郵政核證機關根源證書配對密碼匙之產生程序可使配對密碼匙的獲授權使用者以外人士無法取得私人密碼匙。香港郵政產生核證機關根源證書配對密碼匙，用於發出符合本準則之「智方便」電子證書。「智方便」核證登記辦事處在其處所內的的環境下使用「智方便」系統內的硬體安全模組產生「智方便」電子證書申請人之配對密碼匙。

6.1.2 登記人公開密碼匙交付
「智方便」核證登記辦事處會在產生申請人/登記人的配對密碼匙後產生包含公開密碼匙的「簽發證書要求」(CSR)，並透過系統界面將該要求傳送至香港郵政。

6.1.3 公開密碼匙交付予登記人
香港郵政核證機關根源證書之公開密碼匙可從網頁 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 密碼匙大小
香港郵政之簽署配對密碼匙爲 2048 位元 RSA。「智方便」電子證書的登記人配對密碼匙爲 2048 位元 RSA。

6.1.5 加密模組標準
香港郵政進行之簽署密碼匙的產生、存儲及簽署操作均在硬體加密模組內進行。

6.1.6 密碼匙用途
「智方便」電子證書之密碼匙用於進行數碼簽署。香港郵政核證機關根源證書密碼匙（用於產生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。此外，線上證書狀態應答簽署人之證書用於簽署線上證書狀態應答。

6.2 私人密碼匙保護

6.2.1 加密模組標準
香港郵政核證機關根源證書私人密碼匙利用加密模組產生，其級別至少達到 FIPS140-1 第 4 級。

6.2.2 私人密碼匙多人式控制
香港郵政核證機關根源證書私人密碼匙儲存在可防止篡改加密硬體裝置內。香港郵政採用多人式控制啓動、使用、終止香港郵政私人密碼匙。

6.2.3 私人密碼匙托管
香港郵政並無爲香港郵政核證機關根源證書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 香港郵政私人密碼匙備存
香港郵政核證機關根源證書私人密碼匙的備存，是使用達到 FIPS 140-1 第 4 級保安標準的裝置加密及儲存。香港郵政核證機關根源證書私人密碼匙的備存程序須超過一名人士參與完成。備存的私人密碼匙亦須由超過一名人士啓動。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
香港郵政核證機關根源證書及相關密碼匙使用期不超過二十五年（同見第 4.5 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，均於硬體加密模組內進行。第 4.4 條詳述香港郵政核證機關根源證書公開密碼匙記錄存檔之工作。

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香港郵政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 2.4 條詳述遵守規定之評估。

6.5 生命周期技術保安控制
香港郵政制定控制程序，爲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。

6.6 網絡保安控制
香港郵政核證機關系統有防火牆以及其他接達控制機制保護，其配置只允許根據本準則所載已獲授權之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，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）。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「智方便」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**）。

7.3 線上證書狀態應答結構

通過發佈一個包含主體名稱“Hongkong Post Root CA 2 OCSP Responder”的線上證書狀態應答簽署人證書，香港郵政已授權一個線上證書狀態應答伺服器為根證書 “Hongkong Post Root CA 2” 進行線上證書狀態應答的簽署。通過發佈包含主體名稱“Hongkong Post e-Cert CA 2 - 19 Responder”的線上證書狀態應答簽署人證書，授權線上證書狀態應答伺服器為中繼證書 “Hongkong Post e-Cert CA 2 - 19” 進行線上證書狀態應答的簽署。

線上證書狀態應答結構詳情見**附錄 C**。

8. 本準則管理

本準則之更改一律須經香港郵政批准並公布。有關準則一經香港郵政在香港郵政核證機關網頁 http://www.eCert.gov.hk 或香港郵政儲存庫公布，更改即時生效，並對獲發證書的申請人以及登記人均具約束力。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儘快通知政府資訊科技總監。申請人、登記人及倚據證書人士可從香港郵政核證機關網頁 http://www.eCert.gov.hk 瀏覽此份準則以及其舊有版本。

9. 法律責任和其他業務條款

此部分爲有關「智方便」電子證書之法律陳述，保證和限制條款。

9.1 費用

9.1.1 證書發出或續期費用
「智方便」電子證書免費提供予登記人。

9.1.2 證書查詢費用

香港郵政保留對查詢其證書數據庫確定和收取合理費用之權利。

9.1.3 撤銷或狀態資料查詢費用
香港郵政不會就撤銷證書或倚據證書人士透過使用證書撤銷清單或線上證書狀態應答查看證書的撤銷狀態收取費用。

9.1.4 香港郵政對已獲接收但有缺陷之證書所承擔之責任
儘管下文已列明香港郵政承擔責任之限制，若登記人接收「智方便」電子證書後發現，因「智方便」核證登記辦事處產生的「智方便」電子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，及登記人將此情況立即通知「智方便」核證登記辦事處以便撤銷證書及（如願意）重新發出證書，則「智方便」電子證書將重新發出給登記人。

9.2 財務責任

9.2.1 保險範圍
保單已經備妥，有關證書之潛在或實質責任以及對倚據限額之索償均獲承保。

9.3 業務資料之保密

9.3.1 保密資料範圍
在無意減損其根據條例第 46 條的規定必須承擔之義務之情況下，香港郵政特別將以下類別的資料保密（統稱“保密資料”），並維持合理地控制以防止該等記錄洩露給非受信工作人員。

a) 所有香港郵政擁有及保管的，用於簽署和向登記人發出證書的根源認可核證機關/次認可核證機關的私人密碼匙；
b) 任何業務連續性，應急反應，意外事件及災難恢復計劃；
c) 任何其他用於保護資料保密性，完整性和可用性的安全實務，措施，機制，計劃或程序；
d) 任何根據第 9.4 條作爲隱私資料被香港郵政保管之資料；
e) 任何第 4.4.1 條指明之交易記錄，審計記錄及檔案記錄，包括證書申請記錄以及提交用於輔助申請證書之文件，無論該等申請最後成功或被拒；
f) 交易記錄，財務審計記錄和外部或內部審計記錄及任何審計報告（審計師確認本準則規定之控制的有效性的信函除外）。

9.3.2 不屬於保密的資料

9.3.2.1
公布於「智方便」電子證書內的登記人申請數據被視爲公開且不屬於保密資料。登記人確認所有香港郵政核證機關發出的證書的撤銷數據是公開資料並於儲存庫中公布。

9.3.2.2
私人密碼匙由「智方便」核證登記辦事處保管，香港郵政不會保存任何「智方便」電子證書的私人密碼匙。私人密碼匙由「智方便」核證登記辦事處在其處所內的環境下產生，並儲存在「智方便」系統內的硬體安全模組中。提醒申請人和登記人在申請或續期或接受或使用「智方便」電子證書前，他們應符合「智方便」核證登記辦事處採取適當的有關確保私人密碼匙保密性和安全性的保安措施。

9.4 個人資料隱私保密

9.4.1 隱私保密方案
香港郵政已施行隱私政策，以符合本準則之規定。香港郵政的隱私政策於此網頁公布：https://www.hongkongpost.hk/tc/privacy/index.html。

9.4.2 視作隱私的資料
在證書或證書撤銷清單中不提供於公眾的有關人士之個人資料被視作隱私（統稱“隱私資料”）。

9.4.3 不被視作隱私的資料
證書、證書撤銷清單以及出現在證書、證書撤銷清單內的個人資料不被視爲隱私資料。

9.4.4 使用隱私資料的告知及同意
在得到對象書面同意，或因應適用之法律或法院命令或其他於條例第 46（2）條規定的情況之要求，香港郵政可以使用對象之隱私資料。

9.4.5 倚據司法及行政程序的資料披露
除條例第 46（2）(a）至（d）條之情況，香港郵政不得洩露任何機密資料。無意減損第 46（2）條規定的除外範圍的情況下，香港郵政可以（a）不時向「智方便」核證登記辦事處、承辦商、其他承辦商、顧問或諮詢人披露機密資料，如果該等披露是爲了按照條例規定履行某職能或者爲了條例之目的。或（b）向「智方便」核證登記辦事處披露機密資料，如果該等機密資料與登記人或登記人的證書申請、續期和撤銷有關。

9.5 知識產權
香港郵政、「智方便」核證登記辦事處及承辦商擁有所有有關其數據庫、系統、網頁和包括本準則在內的任何源自香港郵政之公開之知識產權。

商標“香港郵政（HKPost）”和“香港郵政電子證書(Hongkong Post e-Cert)”乃香港郵政之注冊商標。香港郵政可擁有其他未被注冊的商標或服務商標，但其仍爲香港郵政的財產。

證書乃香港郵政獨家擁有之財產。倘若證書按照非獨佔性及免專利的準則下進行完全複製及分發，

則香港郵政允許該等複製和分發的進行。香港郵政保留於任何時候酌情撤銷證書的權利。

9.6 聲明與保證

9.6.1 香港郵政之聲明與保證

9.6.1.1
香港郵政僅向登記人和所有在有效期內實際倚據該類證書的倚據證書人士作出以下保證和聲明（“證書保證”）。

9.6.1.2
在下述限定下，證書保證特別包含保證如下事項：

(A) 一經發出「智方便」電子證書，香港郵政即向任何合理倚據包含於「智方便」電子證書內的資料之人士，或合理倚據可由列載於「智方便」電子證書內的公開密碼匙核實的數碼簽署之人士聲明，香港郵政已根據本準則發出證書。

(B) 一經公布「智方便」電子證書，香港郵政即向任何合理倚據包含於「智方便」電子證書內的資料之人士聲明，香港郵政已向證書辨識之登記人發出證書。

9.6.1.3
對於包含於證書中的其他任何資料，或者由香港郵政，或代表香港郵政編輯、公布或傳播的任何其他資料，香港郵政對於其準確性、真實性、完整性或適當性不做任何保證。

9.6.1.4
香港郵政不保證任何軟件或硬體裝置的質量，功能或性能。

9.6.1.5
由於香港郵政不可控制之原因導致證書無法撤銷，香港郵政不承擔責任。

9.6.2 登記人之聲明與保證

9.6.2.1
各登記人必須親身簽署或確認接受登記人協議。作爲登記人同意的登記人協議的一部分，下列所有承諾與保證皆由或皆視爲由登記人作出，並明確爲了香港郵政、「智方便」核證登記辦事處以及所有倚據證書人士之利益而做出，並在申請、發出以及以其名字發出之證書的有效期內保持真實、完整和準確:

(A) 資料準確性：有義務並且保證在任何時候，在申請「智方便」電子證書或者不時被香港郵政提出要求（不論直接或經由「智方便」核證登記辦事處要求）的情況下向香港郵政和「智方便」核證登記辦事處提供準確和完整之資料以及其他陳述，該等資料包括但不限於發出和接受證書所需要的資料和陳述；

(B) 接受證書：有責任並保證登記人不會使用證書直到登記人審核和核實了證書內數據的準確性；

(C) 證書之使用：有責任並保證僅在遵守所有適用的法律的情況下使用證書，並僅根據登記人協議來使用證書；

(D) 因資料外洩進行的報告和撤銷：一旦發生任何列載於第 4.2.1.4 條的情況，有責任並保證透過「智方便」核證登記辦事處要求香港郵政撤銷證書；以及

(E) 終止使用證書：有責任並保證根據第 4.2.3(b)條，立即停止使用證書及其私人密碼匙。

9.6.2.2
在未限制本準則規定之登記人的其他義務的情況下，登記人僅就於證書內發表的任何失實聲明向合理倚據該聲明之第三方承擔責任。

9.6.2.3
一旦接受證書，登記人即從其接受證書之時開始並在證書的有效期向香港郵政、「智方便」核證登記辦事處及倚據證書人士聲明、保證並負擔以下義務：

(A) 使用對應於包含在證書內的公開密碼匙的私人密碼匙進行的交易是登記人自己的行爲，並且證書在當時以及證書的有效期內已被接受並可正常使用；

(B) 登記人向香港郵政（無論直接或透過「智方便」核證登記辦事處）及「智方便」核證登記辦事處作出的聲明均爲真實，準確和完整；

(C) 所有包含於證書內的資料爲真實，準確和完整；

(D) 證書僅用於經授權和合法的用途，符合本準則規定，並且登記人將於附錄 D 中列載之用途中使用證書；

(E) 登記人同意本準則之條款和條件；

(F) 登記人遵守適用於其國家和地區之法律；

(G) 登記人均已授權「智方便」核證登記辦事處，保管登記人證書之私人密碼匙，及每當登記人進行數碼簽署時，接達其證書之私人密碼匙；

(H) 在使用登記人的證書之私人密碼匙前，登記人已提交「智方便」核證登記辦事處規定的嚴格的驗證程序以核實其「智方便」持有人的身分；

(I) 使用登記人證書中的公開密碼匙對應之私人密碼匙而產生的數碼簽署，乃登記人之數碼簽署。

9.6.3 倚據證書人士之聲明與保證
倚據證書人士接受，爲了合理倚據一份「智方便」電子證書，倚據證書人士必須履行以下所有事項：

(A) 做出合理努力以獲取有關使用電子證書及公匙基建的足夠知識；

(B) 閱讀附錄 D 中所列載電子證書的用途及其使用限制，並透過本準則瞭解香港郵政對於倚據發出的「智方便」電子證書之法律責任的限制；

(C) 通過使用該等人士之名稱，搜索儲存庫以核實登記人是否具有有效的未過期之「智方便」電子證書。停止倚據已經過期之「智方便」電子證書；

(D) 通過參考證書撤銷清單或相關的線上證書狀態應答核實「智方便」電子證書。被撤銷之「智方便」電子證書會在證書撤銷清單或相關的線上證書狀態應答中顯示相應的狀態。停止倚據已經被撤銷之「智方便」電子證書；

(E) 採取任何其他合理的措施將倚據無效的，撤銷的，屆滿的或被拒的「智方便」電子證書產生或以未被授權的方式使用的「智方便」電子證書而產生的數碼簽署所導致的風險最小化；及

(F) 考量以下因素，並僅在根據實際情形確爲合理之情況下才倚據「智方便」電子證書：

(a) 確認一方身分所需要的任何法律要求，保護資料的保密性或隱私性，或根據任何適用的法律，該交易具有的法律可執行性；

(b) 倚據證書人士已經注意到或者應當注意到的，列載於證書和本準測中的所有事實；

(c) 交易的經濟價值；

(d) 因爲在申請、交易或者交流過程中發生驗證錯誤、喪失資料的保密性或私密性造成的潛在損失或潛在損害；

(e) 特定的司法管轄區的法律的適用性，包括列載於與登記人協議或本準則中的司法管轄權；

(f) 倚據證書人士之前與登記人交易的過程，若有；

(g) 貿易慣例，包括與基於計算機的貿易方式有關的的經驗；及

(h) 任何其他可靠或不可靠的標記，以及倚據證書人士知道或注意到的其他關於登記人和/或申請、溝通或交易之事實。

9.7 法律責任限制

9.7.1
登記人有權在由「智方便」核證登記辦事處（如有）提供的機制內酌情決定可使用「智方便」電子證書的交易的最大金額。「智方便」電子證書本身不會就登記人和倚據證書人士之間的交易的最大金額設置限定。

9.7.2
一般免責聲明：在法律允許的最大限度下，香港郵政及「智方便」核證登記辦事處無須對任何人因以下任何事項造成的，或起因於以下任何事項，或與以下任何事項有關聯之任何索賠、訴訟、債務、損失（包含任何直接或間接的損失、任何收益損失、利潤、業務、合約或預期存款）、損害（包含任何直接、特殊、間接或附加的任何性質的損害）或任何損失或開銷承擔任何責任：(a)香港郵政行使本準則中列載之職能或權力；(b)使用或倚據任何「智方便」電子證書及(c)倚據或使用虛假或僞造的並由「智方便」電子證書支援的登記人數碼簽署，而對該證書而言香港郵政已經遵守條例及業務守則中的要求；及(d)以未獲授權或不誠實或欺詐手段使用「智方便」電子證書；(e)「智方便」電子證書中或儲存庫中的任何資料（根據條例第 40 條要求陳述的資料除外）不真實、不準確或不完整。

9.7.3
除列載於條例第 39 條及第 40 條的聲明外，即使本準則中有相反之規定，香港郵政不會向任何人（包括任何登記人，任何倚據證書人士和任何承辦商）作出任何聲明或保證，包括(a)確認證書或儲存庫中（根據條例第 40 條要求確認的資料除外）的任何資料是準確的，正確的或完整的；及(b)透過使用「智方便」電子證書產生的數碼簽署進行的任何交易的有效性和合法性。

9.7.4
除列載於條例第 39 條及第 40 條的聲明外，在法律允許的最大限度下，無論是根據本準則、條例、業務守則或任何登記人協議或者其他法律，香港郵政不會對任何人（包括任何登記人，任何倚據證書人士和任何承辦商）承擔謹慎職責(Duty of Care)。如未有違反列載於條例第 39 條和第 40 條的規定，香港郵政或其僱員在其僱用期內的行爲或疏忽不能被視爲可提起訴訟之疏忽或故意違約行爲。

9.7.5
除了條例第 39 條和第 40 條規定的陳述以及其他依法不能予以排除之陳述與保證之外，香港郵政不提供任何類型的陳述、保證和義務，包括特定目的適用性以及對於提供的未經核實之資料的準確性所做的保證。

9.7.6
若有任何不符或違反本準則或登記人協議或條例第 39 條或第 40 條之情況，對於登記人因爲上述一次或多次不符或違反而遭受損失或損害而提出的可以獲得法律認可且可以證明之索賠，香港郵政就一張「智方便」電子證書的責任而言最高不超過 200,000 港元（總計，如果多過一次不符或違反），或就一張簽發予未滿 18 歲人士的「智方便」電子證書（未成年人士）的責任而言 0 港元。

9.7.7
若有任何不符或違反本準則或列載於條例第 39 條或第 40 條的聲明之情況，對於倚據證書人士因爲上述一次或多次不符或違反而遭受的損失或損害而提出的可以獲得法律認可且可以證明之索賠，香港郵政就一張「智方便」電子證書的責任而言最高不超過 200,000 港元（總計，如多過一次不符或違反），或就一張簽發予未滿 18 歲人士的「智方便」電子證書（未成年人士）的責任而言 0 港元。

9.7.8
承辦商乃由香港郵政按照香港郵政與承辦商之間的獨立合約任命之承辦商，且此任命只以該獨立合約爲條件。本準則不給予承辦商任何額外的權力或要求香港郵政向承辦商承擔額外的義務。至於條例第 39 條和第 40 條中的聲明，承辦商有責任確保其在爲香港郵政履行任何條例中列載之職能的限度內遵守條例中規定的內容。承辦商不是條例第 40 條提及的合理倚據證書內的資料的人士。

9.7.9
所有申請人、登記人、承辦商、倚據證書人士及其他人士、實體和機構同意，除非同意香港郵政於第 9.7 條和第 9.8 條中作出之聲明、保證和條件以及規定的法律責任限制，香港郵政將不會向登記人發出證書，香港郵政也不會提供有關證書的服務，這些條款對合理分攤風險十分必要。

9.7.10
本第 9.7 條和第 9.8 條中的各個條款須獨立詮釋並不得影響本準則其他任何之條款，且除非有明確規定，不得通過參考任何其他條款或由其他條款推斷而受限制。

9.8 關於可追討損失類型的限制及免責聲明

9.8.1
在不影響第 9.7 條免責聲明的情況下，在任何情況下（除詐騙或故意之不正當行爲），香港郵政或「智方便」核證登記辦事處無須就以下任何或全部事項，以及所造成之結果承擔責任：

9.8.1.1
任何間接的、不確定的或附加的損失或損害（即使香港郵政或「智方便」核證登記辦事處已被告知出現此類損失或損害的可能性）；

9.8.1.2
（無論是否視爲直接或間接損失）任何利潤損失、名譽或聲譽上的損失或傷害，機會損失或項目損失；

9.8.1.3
任何死亡或人身傷害（除了任何香港郵政或「智方便」核證登記辦事處的疏忽，“疏忽”參照《管制免責條款條例》（香港法律第 71 章）的定義）；

9.8.1.4
任何數據損失；

9.8.1.5
任何由證書或數碼簽署的使用、傳播、許可使用、履行或不履行引起的或者與之有關的其他任何間接的、附加的或懲罰性損害；

9.8.1.6
任何索賠、訴訟、損失或損害（直接或間接或不確定或特殊），但是因爲倚據條例第 39 條與第 40 條之聲明而造成的除外；

9.8.1.7
任何因倚據證書、證書或儲存庫內的資料而發生的索賠責任，且該等非正常情況是由於申請人或登記人或任何其他人士之欺詐或故意不正當行爲而導致的；

9.8.1.8
任何因未按照本準則使用證書引起的責任；

9.8.1.9
任何因使用無效的證書（過期或已撤銷）引起的責任；

9.8.1.10
任何因使用證書超過適用的使用限制而引起的責任；

9.8.1.11
任何因安全性、可用性、產品的完整性而引起的責任（包括申請人/登記人使用的硬體和軟件）；

9.8.1.12

任何由證書之私人密碼匙外洩引起的責任。

9.8.2 非商品供應

特此澄清，登記人協議並非任何性質之商品之供應合約。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、所有權或利益均不得轉讓於登記人，登記人僅有權申請發出證書及根據概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或服務；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或服務的陳述或保證。

9.8.3 提出索賠的時限

在不影響第 9.7 條和第 9.8 條及於本準則其他地方規定之免責聲明和限制的情況下，任何登記人或倚據證書人士或任何其他人士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「智方便」電子證書相關，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。

9.8.4「智方便」核證登記辦事處、香港郵政署、承辦商及其各自之人員

香港政府或香港政府之任何職員、僱員港或其代理人（除了香港郵政）均非登記人協議之簽約人。登記人及倚據證書人士必須承認，據登記人及倚據證書人士所知，香港政府、香港政府的任何職員、僱員或代理人（包括「智方便」核證登記辦事處和香港郵政的職員、僱員和代理人）（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認可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。各登記人及倚據證書人士向香港政府、其職員與僱員以及代理人（包括「智方便」核證登記辦事處和香港郵政的職員、僱員和代理人）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）、並與香港郵政履行登記人協議或由香港郵政作爲認可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這些機構及個人免受此等法律行動。

9.8.5 欺詐責任

香港郵政因欺詐造成之責任不屬 本準則規定的任何限定或除外規定範圍之內，任何登記人協議或由香港郵政發出之證書亦不受任何此等規定之限制或被任何此等規定限制或免除。

9.8.6 證書通知，限制及倚據限額

在不影響本準則餘下條款約束力的情況下，香港郵政發出之「智方便」電子證書應認作已包括本準則第 9.6 條至第 9.15 條之規定。

9.9 賠償

一旦接受或使用或倚據證書，各登記人和倚據證書人士即同意賠償香港郵政以及香港政府，及其（包括「智方便」核證登記辦事處和香港郵政）職員、僱員、代理人和承辦商因任何責任導致的可能會給香港郵政及上述人士造成之任何責任，任何損失或損害以及債務，及任何類別的索賠、

法律程序、成本、費用和開支，包括全額賠償之法律費用，並承諾香港郵政以及香港政府，及其（包括「智方便」核證登記辦事處和香港郵政）職員、僱員、代理人和承辦商免受上述責任、損失、損害或費用之損害。該等責任、損失、損害或費用等是由於該等人士在使用或公布證書的過程中有如下行爲而造成：(i) 爲獲取或使用證書而對重要事實進行了虛假陳述或者未能陳述重要事實（無論此類虛假陳述或遺漏是有意或是由於疏忽或草率造成）；(ii) 違反登記人協議、本準則或任何適用的法律；(iii) 因該等人士而非因香港郵政的疏忽導致資料外洩或未授權使用證書或私人密碼匙；或 (iv) 誤用證書或私人密碼匙。

9.10 期限與終止

9.10.1 期限

本準則及其任何修改由香港郵政在香港郵政核證機關網站 http://www.eCert.gov.hk 或在儲存庫公布時生效，並將維持有效直至根據本準則第 9.10 條終止爲止。

9.10.2 終止

本準則可經不時之修改並維持有效，直至被新的版本所取代或者根據本準則第 9.10 條終止爲止。

9.10.3 終止的生效與效力續存

本準則終止的條件和效力將在其終止時於香港郵政的儲存庫（http://www.eCert.gov.hk）予以通告。該通告中將簡述不受終止之影響而在終止後持續有效之條款。保護商業秘密和個人隱私之責任終止後繼續有效，對於已經存在之證書中的條款和條件將在該證書有效期之剩餘期間內繼續有效。

在此特別聲明，香港郵政可在無需得到任何人之同意的情況下，終止本準則。

9.11 對參與者的個別通知與溝通

香港郵政接受通過電子形式或信件形式寄往本準則第 1.3 條規定地址與本準則有關的通知。當收到來自香港郵政之有效認收信息時，通知的發出者可以藉此確認其溝通已經生效。

9.12 修改

9.12.1

所有對於本準則的修改由有權決定此等修改的香港郵政公布。**在此特別聲明，香港郵政可在無需得到任何人之同意的情況下，修改本準則。**有關準則一經香港郵政在香港郵政核證機關網頁 http://www.eCert.gov.hk 或香港郵政儲存庫公布，更改即時生效，並對所有申請人、登記人、「智方便」核證登記辦事處、倚據證書人士、承辦商以及在登記人協議中被視為第三方人士之其他人士均具有約束力（無需事先考慮或取得任何該等人士之同意）。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儘快通知政府資訊科技總監。此份準則以及其舊有版本可在香港郵政核證機關網頁 http://www.eCert.gov.hk 瀏覽。**對於那些不同意本準則前述更改的登記人，自這些修改生效起一個月內，可以根據第 4.2.2.1 條規定向香港郵政發出通知要求停止使用「智方便」電子證書並透過「智方便」核證登記辦事處撤銷「智方便」電子證書。在上述的一個月期限內若無任何來自登記人的通知，將視作登記人同意這些更改。**

9.12.2

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。在上述規定約束下，所有其他改變都須獲得登記人協議各方的同意。登記人協議的變更 (不論是由香港郵政單方進

行或登記人與香港郵政達成協議進行) 可在無需取得任何第三方的同意下，進行上述任何修改。

9.12.3
根據本準則之條款任何一方（不論是由香港郵政單方進行或登記人與香港郵政達成協議進行）終止登記人協議、終止或撤銷任何「智方便」電子證書無需取得任何第三方同意。

9.12.4 已經採取合理措施以確保該等第三方會透過公布本準則而瞭解到本準則第 9.12 條。

9.13 爭議之解決程序
香港郵政關於本準則範圍內之事宜之決定為最終決定。如有索償，請送交下列地址：

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

9.14 管轄法律
本準則受香港法律規管並依香港法律解釋。該等法律選擇是爲了確保本準則解釋一致性，而與香港郵政數碼證書的所在地和使用地無關。

雙方均同意服從香港法院的專屬司法管轄權，以解決因本準則或登記人協議引起的或與之相關的任何爭議。

9.15 完整協議

9.15.1
本準則應當持續在符合商業習慣、商業上合理的條件以及本準則涉及之產品或服務的目標用途之範圍內進行解釋。在解釋本準則時，各方應當考慮到香港郵政的服務和產品範圍和應用以及其在商業交易中適用之誠信原則。雖有前述之規定，由香港郵政發出的用於其他類型證書的核證作業準則將不被用於解釋本準則的規定。

9.15.2
本準則中的標題、副標題以及其他章節僅爲方便參考之用，而不應用於解釋、解讀或執行本準則的任何規定。

9.15.3
本準則的附錄和定義對所有人士而言爲本準則整體之不可分離且具有約束力之組成部分。

9.15.4
如果/當本準則（包括不時的修改）與其他規則、指南或合約相衝突時，本準則（除非本準則的條款被條例所禁止）優先適用於登記人和其他當事人並具有約束力。如果本準則的條款之間存在衝突，或與香港郵政有關的其他文件存在衝突時，香港郵政可酌情決定優先適用有利於香港郵政、保留香港郵政最佳利益的條款，約束有關的各方。

9.16 轉讓
沒有香港郵政之書面同意，本準則之各方不能轉讓其在本準則或者適用的協議項下的任何權利或

義務。

9.17 可分割性

9.17.1
如果本準則的任何規定或其應用由於任何原因在某些程度上被認定爲無效或者無強制力的，本準則的剩餘內容將維持有效，並爲了能在最大可能限度內事實各方最初之目的而進行解釋。

9.17.2
本準則內的每一條限制責任或免責聲明或損害排除之條款，均爲可分割的且不受其他條款約束，並可按此執行。

9.18 執行（律師費和放棄權利）

香港郵政保留向任何與在本準則第 9.9 條規定的行爲有關的一方尋求損害賠償和法律費用之權利。除非本準則規定了時間架構，任何一方延遲或者疏於行使任何基於本準則之權利、救濟或權力，將不會妨礙或者被解釋爲放棄該等權利、救濟或權力。任何一方放棄本準則規定之任何違約或者義務，不得被解釋爲對其他任何後續毀約或義務的棄權。香港郵政與本準則各方之間的雙邊協議可以對本準則之執行包含追加規定。

9.19 不可抗力

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

9.20 其他規定

9.20.1
本準則對適用本準則的各方之繼承者、執行者、後代、代表者、管理者和受讓人（不論是明示還是暗示形式）均有約束力。

9.20.2 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。

9.20.3 受信關係

無論在任何時候，香港郵政、「智方便」核證登記辦事處或承辦商並非登記人或倚據證書人士之代理人、受信人、收托人或其他代表。登記人或倚據證書人士無權以合約或其他方式約束香港郵政、「智方便」核證登記辦事處或承辦商承擔代理人、受信人、受托人或其他代表的責任。

9.20.4 詮釋

本準則中英文本措詞詮釋若有歧異，以英文本爲準。

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佈或在某儲存庫內公佈；
  (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佈或在某儲存庫內公佈；或
  (iii) 以其他方式顯示承認該證書；

“申請人” 指自然人並已申請「智方便」電子證書。「智方便」電子證書一旦成功申請及發出，申請人即被稱為登記人。

“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。

“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佈無效之公開密碼匙中繼證書之資料。

“證書”或**“「智方便」電子證書”**指符合以下所有說明之紀錄 ：
a) 由香港郵政發出，其目的爲支持數碼簽署用以確認該證書上標明之人士確實爲有權使用與包含在證書中的公共密碼匙相對之私人密碼匙之人士；
b) 識別香港郵政爲發出其之認可核證機關；
c) 指名或識別獲發紀錄之人士；
d) 包含了獲發紀錄人士之公開密碼匙；並
e) 經發出紀錄的香港郵政作爲核證機關簽署。

“核證機關”指向他人(可以為另一核證機關)發出證書者。

“核證作業準則”或**“準則”**指本文件及其所有附錄。

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

“簽發證書要求”指「智方便」核證登記辦事處收到申請人的「智方便」電子證書申請後生成的訊息，並通過「智方便」系統發送給香港郵政，以申請證書。
“實務守則”指由政府資訊科技總監在條例第33條下頒布之認可核證機關實務守則。

“合約”指香港郵政不時與承辦商簽訂的外判合同，在香港郵政的監督和管理下代表香港郵政履行本作業準則所規定的全部或任何職能。

“承辦商”指香港郵政不時訂立的合約之承辦商；以及該承辦商的所有分辦商。

“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。

“身份證”指根據《人事登記條例》第 177 章發出的身份證。

“香港郵政”指郵政署長為該條例認可的核證機關。

“香港郵政核證機關系統”指香港郵政用以執行核證機關功能的電腦硬件，軟件和程序。

“硬體安全模組” 指用於中央存儲和管理證書以及保護密碼匙不被導出或複制的硬件安全設備。

“「智方便」持有人” 指在「智方便」核證登記地點獲得「智方便」的人，並且其「智方便」在「智方便」系統中仍然有效。

“港元”指香港之合法貨幣。

“香港”指中華人民共和國香港特別行政區。

“智方便”指香港政府提供給香港居民進行電子交易的電子身分。在本準則中，「智方便」指的是根據3.1.1節所獲得的「智方便」的版本。

“「智方便」核證登記地點”指「智方便」核證登記辦事處提供之附有特定裝置的指定場所之登記地點，該登記地點提供給香港居民親身註冊「智方便」，其「智方便」版本符合資格申請「智方便」電子證書。

“「智方便」系統”指由政府（通過「智方便」核證登記辦事處委任的承辦商）開發和管理的系統，該系統向香港居民提供「智方便」功能，包括註冊，使用和帳戶維護。

“「智方便」核證登記辦事處”指第1.2.2節中提及的「智方便」核證登記辦事處。

“入境事務處”指香港特區政府入境事務處。

“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) 。

“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爲獲發該證書的人的資訊，直接通知該人或通過「智方便」核證登記辦事處間接通知該人；或
(b) 將該證書將會包含的關於在該證書內指名或識別爲獲發該證書的人的資訊，直接通知該人或通過「智方便」核證登記辦事處間接通知該人，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。

“OCSP”指線上證書狀態通訊規約，用於檢查證書的狀態。

“條例”指香港法例第 553 章《電子交易條例》。

“組織”指除個人之外之任何實體。

“公匙基建”指公開密碼匙基礎建設

“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”指代表香港郵政履行核證登記職能，在發出「智方便」電子證書前核實申請人身份之機構。

“倚據限額”指第 9.7 條規定的倚據「智方便」電子證書之金額限額。

“**倚據證書人士**” 指合理地倚據「智方便」電子證書中所包含之資料之人士，但該人士必須遵守第 9.6.3 條規定之聲明保證。

“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。

“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。

“**登記人參考編碼**”指香港郵政系統產生的一個登記人參考編碼。

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

“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) 已授權「智方便」核證登記辦事處持有與該證書公開密碼匙相對應之私人密碼匙。

注： 與本準則中提及之私人密碼匙相關之“持有”指處在某人之控制之下，以致僅有證書中指名或識別之人方能使用該私人密碼匙。

“**登記人協議**” 就「智方便」電子證書而言，指香港郵政和該證書登記人之協議，其中包括了「智方便」電子證書的《登記人條款及條件》以及本準則。

“穩當的系統” 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) 可用性和可靠性達到了合理水準，且可以在合理的期間內保證正確之運作模式；

(c) 合理地適合與執行其原定功能；及

(d) 依循廣爲接受之安全原則。

解釋原則

2.1. 在本準則中，除非前後文另有所指，必須遵從以下之解釋規則。

(a) 提及成文法律或者成文法律性條款之內容應被解釋爲引用該等成文法律或者成文法律性條款之不時之替代、修訂、修改或重新生效，並且應該包括根據該等條款所做出之附屬性立法；

(b) 詞語引用之單數形式包括複數形式，反之亦然。詞語引用之性別包括所有性別。詞語中的“人”包括任何個人、企業、公司或未經公司設立程序之實體（不論是否設立或是否完成了公司設立程序）；

(c) 條款之標題僅爲便於參考之目的，對於本準則之解釋沒有影響；

(d) 提及某一文件時應：

(i) 包括所有附加於該文件之附件、附錄和添附文件；以及

(ii) 包括不時被修改或補充後之該文件。

(e) 提及“登記人”或“申請人”或“倚據證書人士”或“承辦商”時應包括該等人之經批准的受讓人、所有權繼承人或者任何在此之下享有衍生權利之人；

(f) 提及“香港郵政” 或“「智方便」核證登記辦事處”時，應包括其受讓人、所有權繼承人或者任何在此之下享有衍生權利之人，不論該等人士是否在相關條款中有被獨立提及；

(g) 提及條文、附錄或附件時，除特別聲明外，應指本準則之條文、附錄或者附件；

(h) 提及“法律”、“法規”時應包括任何具有法律之效力之憲法性條款、條約、公約、條例、附屬立法、命令、規則和法規以及任何民事法、普通法以及衡平法之法律規則；

(i) 一天中的某個時間應指香港時間；

(j) 提及一日應指公曆日；提及工作日應指除星期六、根據《公眾假期條例》（第149章）的所有公眾假期、及發出黑色暴雨警告信號或懸掛八號或以上熱帶氣旋信號的日子以外的任何公曆日；提及一個月或一個月期間是指一個公曆月；

(k) 詞語引用某一整體的，應被看作包含了該整體之各部分；

(l) “包括”這一詞語不論是否明確做出該種規定都應表示包括但不限於；

(m) 詞語或者表現形式如果在本準則中被定義或被引用其他定義，該等詞語或表現形式延伸至該其在語法上之變體以及與之同源之表現形式；

(n) 提及“書面”時應包括打字、印刷、微影、攝影、傳真或者以電子郵件方式進行之溝通之

印刷版本，也包括以其他可以辨別內容之形式呈現或者重現文字；及

(o) 在數字後提及“章”時代表香港法律之相關章節；

2.2. 本準則之任何內容都不得被用於限制、損害或者干涉任何香港郵政受法律賦予或者依據法律履行的權力與責任，以及香港郵政就此等權力與責任之行使或執行。

附錄 B - 香港郵政「智方便」電子證書格式

本附錄詳述由中繼證書"Hongkong Post e-Cert CA 2 - 19"根據本核證作業準則簽發的「智方便」電子電子證書格式。

A. 「智方便」電子證書格式

欄位名稱		欄位內容	
		香港郵政「智方便」電子證書	發出予未滿18歲人士的 香港郵政「智方便」電子證書
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	
發出人名稱 (Issuer name)		cn=Hongkong Post Root CA 2 -19 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=[香港身份證姓名]（附註1） ou=[登記人參考編號]（附註2） o=Hongkong Post iAM Smart-Cert c=HK	cn=[香港身份證姓名]（附註1） ou=[登記人參考編號]（附註2） o= Hongkong Post iAM Smart-Cert (Minor)（附註3） c=HK
主體公開密碼匙資料 (Subject public key info)		算式識別 (Algorithm ID)：RSA 公開密碼匙 (Public key)：密碼匙長度為2048位元	
發出人識別名稱 (Issuer unique identifier)		未使用	
登記人識別名稱 (Subject unique identifier)		未使用	
標準延伸欄位 (Standard extension)（附註4）			
機關資料查詢 (Authority Information Access)	核證機關發出人 (Certification Authority Issuer)	[發出人公開證書的URL]	
	線上證書狀態應答 (OCSP)	[線上證書狀態應答URL]（附註9）	

欄位名稱		欄位內容	
		香港郵政「智方便」電子證書	發出予未滿18歲人士的 香港郵政「智方便」電子證書
機關密碼匙識別名稱 (Authority key identifier)	發出人 (Issuer)	cn=Hongkong Post e-Cert CA 2 o=Hongkong Post l=Hong Kong s=Hong Kong c=HK	
	序號 (Serial number)	[從發出人處獲取]	
密碼匙使用方法 (Key usage)		數碼簽署，不可否認 **（此欄為“關鍵”欄位）**	
證書政策 (Certificate policies)		Policy Identifier = [物件識別碼]（附註 5） Policy Qualifier ID = CPS Qualifier : [核證作業準則的URL] Policy Identifier = 1.3.6.1.4.1.16030.1.4（附註6） Policy Qualifier Id = CPS Qualifier = [核證作業準則的URL]	Policy Identifier = [物件識別碼]（附註5） Policy Qualifier Id = CPS Qualifier = [核證作業準則的URL]
主體別名 (Subject alternative name)	DNS	[經加密的香港身份證號碼]（附註7）	
發出人別名 (Issuer alternative name)		未使用	
基本限制 (Basic constraints)	主體類型 (Subject type)	最終實體	
	路徑長度限制 (Path length constraint)	無	
延伸密碼匙使用方法 (Extended key usage)		SSL Client	
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. 申請人姓名格式： 英文格式 - 姓氏（大寫）+ 名（例如 CHAN Tai Man David）
2. 登記人參考編號： 10 位數字
3. “iAM Smart-Cert (Minor)”表示 申請人於獲發出證書時未滿 18 歲（見本核證作業準則第 3.1.3 條）。
4. 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。
5. 本欄已包括本核證作業準則的物件識別碼 (Object Identifier, OID)。關於本準則的物件識別碼，請參閱本準則第 1.1 條。
6. 本欄已增加一個支持 Adobe PDF 簽名的物件識別碼。
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為一雜湊數值(以 **cert_hkid_hash** 表示)後，存入證書：

$$cert\_hkid\_hash = \text{SHA-256}\left(\text{RSA}_{privatekey,\ sha\text{-}256}\left(hkid\_number\right)\right)$$

*SHA-256*為一雜湊函數而*RSA*則為簽署函數

8. 證書撤銷清單分發點 URL 為 http://crl1.eCert.gov.hk/crl/eCertCA2-19CRL1_<xxxxx>.crl，由中繼證書“Hongkong Post e-Cert CA 2 - 19”所發出，其中 <xxxxx> 為 經香港郵政系統產生，包含 5 個數字或字符的字串。香港郵政會公佈各「分割式證書撤銷清單」。已撤銷證書的資料，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。

9. 線上證書狀態通訊規約應答伺服器的 URL 為 http://ocsp1.eCert.gov.hk

附錄 C - 香港郵政證書撤銷清單(CRL) 、香港郵政授權撤銷清單(ARL)及香港郵政線上證書狀態應答(OCSP) 格式

本附錄 C 詳述有關由中繼證書"Hongkong Post e-Cert CA 2 - 19"所發出的證書撤銷清單的更新及公佈安排和其格式，以及由"Hongkong Post Root CA 2"所發出的授權撤銷清單(ARL) 的更新及公佈安排和其格式。

此外，通過發佈一個包含主體名稱為“Hongkong Post Root CA 2 OCSP Responder”的線上證書狀態通訊規約簽署人證書，香港郵政已授權一個線上證書狀態通訊規約應答伺服器為根源證書“Hongkong Post Root CA 2”進行線上證書狀態通訊規約的簽署。通過發佈一個包含主題名稱為“ Hong Kong Post e-Cert CA 2-19 OCSP Responder”的線上證書狀態通訊規約簽署人證書，亦授權一個線上證書狀態通訊規約應答伺服器為中繼證書“ Hong Kong Post e-Cert CA 2-19”進行線上證書狀態通訊規約的簽署。除此之外，線上證書狀態通訊規約應答伺服器獲分配了一個唯一的物件識別碼 OID“ 1.3.6.1.4.1.16030.1.6”，指定於線上證書狀態通訊規約簽署人證書的“證書策略”欄位。在本附錄 C 的最後章節，還提供了線上證書狀態應答的格式。

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「智方便」電子證書的資訊：

a) **「分割式證書撤銷清單」 (Partitioned CRL)** 包含分組的已撤銷證書的資料。公眾可於下述位址(URL)獲取相關的「分割式證書撤銷清單」：

> 「智方便」電子證書：
> 由中繼證書"Hongkong Post e-Cert CA 2 - 19"所發出 http://crl1.eCert.gov.hk/crl/eCertCA2-19CRL1_<xxxxx>.crl，其中 <xxxxx> 為包含 5 個數字或字符的字串。

b) **「整體證書撤銷清單」 (Full CRL)** 包含由中繼證書"Hongkong Post e-Cert CA 2 - 19"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」：

> http://crl1.eCert.gov.hk/crl/eCertCA2-19CRL1.crl; 或 ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post e-Cert CA2 - 19 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佈。在不能預見及有需要的情 況下，香港郵政可不作事前通知而更改上述證書撤銷清單的更新及公佈的時序。香港郵政也會在有需要及不作事前通知的情況下，於香港郵政網頁 http://www.eCert.gov.hk 公佈補充證書撤銷清單。

由中繼證書"Hongkong Post e-Cert CA 2 - 19"根據本準則發出的分割式及整體證書撤銷清單格式:-

標準欄位 (Standard Fields)	子欄位 (Sub-fields)	分割式證書撤銷清單欄位內容	整體證書撤銷清單欄位內容	備註
版本 (Version)		v2		此欄顯示證書撤銷清單格式的版本為 X.509 第二版
簽署算式識別 (Signature algorithm ID)		Sha256RSA		此欄顯示用以簽署證書撤銷清單的算法的識別碼
發出人 (Issuer name)		cn=Hongkong Post e-Cert CA 2 - 19, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK		此欄顯示簽署及發出證書撤銷清單的機構
此次更新 (This update)		[UTC 時間]		此欄顯示本證書撤銷清單的發出日期 (是次更新)
下次更新 (Next update)		[UTC 時間]		表示下次證書撤銷清單將於顯示的日期或之前發出 (下次更新)，而不會於顯示的日期之後發出。根據核證作業準則的規定，證書撤銷清單是每天更新及發出
撤銷證書 (Revoked certificates)	用戶證書 (User certificate)	[證書序號]		此欄列出已撤銷證書的證書序號
	撤銷日期 (Revocation date)	[UTC 時間]		此欄顯示撤銷證書的時間
	證書撤銷清單資料延伸欄位 (CRL entry extensions)			
	原因代碼 (Reason code)	[撤銷理由識別碼]		（附註 1）
標準延伸欄位 (Standard extension) （附註 2）				
機關密碼匙識別名稱 (Authority key identifier)	發出人 (Issuer)	cn=Hongkong Post Root CA 2 o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK		此欄提供有關資料以識別用作簽署證書撤銷清單的私人密碼匙的配對公開密碼匙。
	序號 (Serial number)	[發出人證書的序號]		此欄顯示發出人證書的序號
證書撤銷清單號碼 (CRL number)		[由核證系統產生 – 每一分割式證書撤銷清單有其自己的序列]		此欄顯示證書撤銷清單的編號，該編號以順序形式產生。

標準欄位 (Standard Fields)	子欄位 (Sub-fields)	分割式證書撤銷清單欄位內容	整體證書撤銷清單欄位內容	備註
發出人分發點 (Issuer distribution point)		分發點名稱=分割式證書撤銷清單 URL 只存有用户證書=是 只存有核證機關證書=否 間接的 CRL=否 **（此欄為“關鍵”欄位）**	[未使用]	本欄位祇為分割式證書撤銷清單使用。

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

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)

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)		

標準欄位 (Standard fields)	子欄位 (Sub-fields)	授權撤銷清單欄位內容	備註
	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 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）**	

根據本準則發出的線上證書狀態應答(OCSP response)格式:-

香港郵政線上證書狀態通訊規約應答伺服器只支持基本的線上證書狀態應答類型。一個明確的線上證書狀態應答數據由以下組成：

標準欄位 (Standard Fields)	子欄位(Sub-fields)	子欄位(Sub-fields)	欄位內容	備註
應答數據 (Response data)	版本(Version)		v1 (0x0)	
	應答伺服器識別 Responder ID	by key 憑密碼匙	[應答伺服器的公匙 SHA-1 雜湊值]	
	Produced At 產生於		[Generalized 時間]	此應答簽署的時間 (GMT+0).
	Sequence of Single Response 單一應答的序列			
	Single Response 單一應答	Certificate ID 證書識別	[要求的證書識別名稱]	要求的證書識別名稱包含： • 雜湊函數識別 • 發出人主體名稱的雜湊值 • 發出人公匙的雜湊值 • 證書序號
		證書狀態 (Certificate status)	[證書的狀態]	有效、撤銷（附有日期、時間(GMT+0)和撤銷原因代碼（附註 1））或未知
		本次更新 This update	[Generalized 時間]	證書正確狀態的最近日期和時間 (GMT+0).
		下次更新 Next update	[Generalized 時間]	更新證書狀態的日期和時間 (GMT+0).
簽署算式識別 (Signature algorithm ID)			sha256RSA	用於簽署此應答的算法
簽署(Signature)			[簽署數據]	應答的簽名
證書(Certificate)			[應答伺服器簽署人證書的數據]	應答伺服器的簽署人證書

附註：

1. 以下為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為 “非關鍵” (Non-Critical) 延伸欄位。

附錄 D - 香港郵政「智方便」電子證書 – 服務摘要

要點	「智方便」電子證書
登記人	持有「智方便」的香港居民（請參閱第 3.1.1 條）
證書之授權用戶	與登記人相同
倚據限額	• 每張「智方便」電子證書HK$200,000，或 • 每張發出予未滿18歲人士的「智方便」電子證書HK$0 （請參閱第 9.7.6 條及 9.7.7 條）
認可證書	是
配對密碼匙長度	2048 位元 RSA
產生配對密碼匙	由「智方便」核證登記辦事處代製產生
於申請「智方便」電子證書時核實身分	如第 4.1.1 條所述
證書用途	不可否認的數碼簽署
證書內包含登記人的資料	• 登記人的英文姓名； • 登記人香港身份證號碼的雜湊數值 (hash value)；及 • 登記人參考編號（由香港郵政系統產生）
登記及行政費用	免費
證書有效期	一年

附錄 E - 核證機關根源證書的有效期

根源證書名稱	有效期	備註
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
Hongkong Post e-Cert CA 2 – 19	2019年7月29日 至 2034年7月29日	此中繼證書由2020年10月7日起開始發出「智方便」電子證書給申請者。