

Hongkong Post Bank-Cert

香港郵政銀行證書

以香港郵政署長

根據電子交易條例作為認可核證機關

之

銀行證書核證作業準則



日期：二零零四年一月十二日

物件識別碼：1.3.6.1.4.1.16030.1.2.1

目錄

前言.....	4
1. 引言.....	5
1.1 概述.....	5
1.2 社區及適用性.....	5
1.2.1 核證機關.....	5
1.2.2 最終實體.....	5
1.2.3 登記人之級別.....	6
1.2.4 證書之期限.....	6
1.2.5 在香港郵政批核之處所進行申請.....	6
1.3 聯絡資料.....	6
1.4 處理投訴程序.....	7
2. 一般規定.....	7
2.1 義務.....	7
2.1.1 核證機關之義務.....	7
2.1.2 核證登記機關之義務及責任.....	7
2.1.3 登記人之義務.....	7
2.1.4 倚據證書人士之義務.....	8
2.2 其他規定.....	8
2.2.1 合理技能及謹慎.....	8
2.2.2 非商品供應.....	9
2.2.3 法律責任限制.....	9
2.2.4 香港郵政對已接受但有缺陷之證書所承擔之責任.....	11
2.2.5 登記人轉讓.....	11
2.2.6 陳述權限.....	11
2.2.7 更改.....	11
2.2.8 保留所有權.....	12
2.2.9 條款衝突.....	12
2.2.10 受信關係.....	12
2.2.11 交相核證.....	12
2.2.12 財務責任.....	12
2.3 解釋及執行（管轄法律）.....	12
2.3.1 管轄法律.....	12
2.3.2 可分割性、尚存、合併及通知.....	12
2.3.3 爭議解決程序.....	12
2.3.4 詮釋.....	12
2.4 收費.....	12
2.5 公開發表資料及儲存庫.....	12
2.5.1 證書儲存庫控制.....	13
2.5.2 證書儲存庫進入要求.....	13
2.5.3 證書儲存庫更新週期.....	13
2.6 遵守規定之評估.....	13
2.7 機密性.....	13
3. 鑑別及認證.....	13
3.1 首次申請.....	13
3.1.1 名稱類型.....	13

3.1.2 名稱需有意義	14
3.1.3 詮釋各個名稱規則	14
3.1.4 名稱獨特性	14
3.1.5 名稱申索爭議決議程序	14
3.1.6 侵犯及違反商標註冊	14
3.1.7 證明擁有私人密碼匙之方法	14
3.1.8 機構申請人身份認證	14
3.1.9 個人申請人身份認證	15
3.2 證書續期	15
3.2.1 銀行證書（個人）	15
3.2.2 銀行證書（機構）	15
3.2.3 已續期銀行證書之有效期	15
4 運作要求	15
4.1 證書申請	15
4.2 發出證書	16
4.3 接受及公佈證書	16
4.4 證書撤銷	16
4.4.1 撤銷	16
4.4.2 撤銷程序請求	17
4.4.3 服務承諾及證書撤銷清單更新	18
4.4.4 撤銷效力	19
4.5 電腦保安審核程序	19
4.5.1 記錄事件類型	19
4.5.2 處理記錄次數	19
4.5.3 審核記錄之存留期間	19
4.5.4 審核記錄之保護	19
4.5.5 審核記錄備存程序	19
4.5.6 審核資料收集系統	19
4.5.7 事件主體向香港郵政發出通知	19
4.5.8 脆弱性評估	19
4.6 記錄存檔	20
4.6.1 存檔記錄類型	20
4.6.2 存檔保存期限	20
4.6.3 存檔保護	20
4.6.4 存檔備存程序	20
4.6.5 電子郵戳	20
4.7 密碼匙變更	20
4.8 災難復原及密碼匙資料外泄計劃	20
4.8.1 災難復原計劃	20
4.8.2 處理密碼匙資料外泄計劃	21
4.8.3 密碼匙的替補	21
4.9 核證機關終止服務	21
4.10 核證登記機關終止服務	21
5. 實體、程序及人員保安控制	21
5.1 實體保安	21
5.1.1 選址及建造	21
5.1.2 進入控制	21

5.1.3 電力及空調.....	21
5.1.4 自然災害.....	21
5.1.5 防火及保護.....	22
5.1.6 媒體存儲.....	22
5.1.7 場外備存.....	22
5.1.8 保管印刷文件.....	22
5.2 程序控制.....	22
5.2.1 受信職責.....	22
5.2.2 港郵政與核證登記機關之間的文件及資料傳遞.....	22
5.2.3 年度評估.....	22
5.3 人員控制.....	22
5.3.1 背景及資格.....	22
5.3.2 背景調查.....	22
5.3.3 培訓要求.....	22
5.3.4 向人員提供之文件.....	23
6. 技術保安控制.....	23
6.1 產生及安裝配對密碼匙.....	23
6.1.1 產生配對密碼匙.....	23
6.1.2 登記人公開密碼匙交付.....	23
6.1.3 公開密碼匙交付予登記人.....	23
6.1.4 密碼匙大小.....	23
6.1.5 加密模組標準.....	23
6.1.6 密碼匙用途.....	23
6.2 私人密碼匙保護.....	23
6.2.1 加密模組標準.....	23
6.2.2 私人密碼匙多人式控制.....	23
6.2.3 私人密碼匙托管.....	23
6.2.4 香港郵政私人密碼匙備存.....	24
6.3 配對密碼匙管理其他範疇.....	24
6.4 電腦保安控制.....	24
6.5 生命周期技術保安控制.....	24
6.6 網絡保安控制.....	24
6.7 加密模組工程控制.....	24
7. 證書及證書撤銷清單結構.....	24
7.1 證書結構.....	24
7.2 證書撤銷清單結構.....	24
8. 準則管理.....	24
附錄 A - 詞彙.....	25
附錄 B - 香港郵政銀行證書格式.....	28
附錄 C - 香港郵政證書撤銷清單(CRL)格式.....	32
附錄 D - 香港郵政銀行證書 — 服務摘要.....	34
附錄 E - 香港郵政銀行證書核證登記機關名單.....	35

本文之版權屬香港郵政署長所有。未經香港郵政署長明確認可，不得複製本文之全部或部份內容。

前言

香港法例第 553 章之電子交易條例(「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，其身份為**香港郵政**。

根據條例，香港郵政作為認可之核證機關，負責使用穩當系統發出、暫時吊銷或撤銷及利用公開儲存庫公佈已認可及接受之數碼證書作為在網上進行穩妥的身份辨識。**根據本核證作業準則發出的證書，在本核證作業準則內稱為“證書”或“銀行證書”。**

根據條例，香港郵政可以採取任何合宜舉措以履行核證機關職能及提供核證機關服務。而根據資訊科技署署長頒布之認可核證機關作業守則，香港郵政可以指定代理人或分包商進行其若干或所有作業。

香港郵政可合宜地指定若干金融機構為代理人，履行香港郵政作為認可核證機關之若干職能。在本銀行證書核證作業準則中，該等機構稱為銀行證書核證登記機關，或者，核證登記機關及其職能已列載於本核證作業準則中。附錄 E 列載核證登記機關之清單。香港郵政透過該等核證登記機關發出兩類銀行證書予個人(銀行證書(個人))及某些機構之成員或僱員(銀行證書(機構))。香港郵政對其代理人即核證登記機關履行香港郵政作為認可核證機關有關簽發及撤銷銀行證書之職能或提供服務的行為負責。

本核證作業準則列載香港郵政銀行證書(個人)及香港郵政銀行證書(機構)之作業標準，其結構如下：

- 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 條列載申請及身份確認程序
- 第 4 條概述運作要求
- 第 5 條介紹保安監控措施
- 第 6 條列載如何產生及監管公開/私人配對密碼匙
- 第 7 條簡介技術要求
- 第 8 條概述如何管理本核證作業準則
- 附錄 A 載有詞彙表
- 附錄 B 載有香港郵政銀行證書格式
- 附錄 C 載有香港郵政證書撤銷清單格式
- 附錄 D 載有香港郵政銀行證書服務摘要
- 附錄 E 載有香港郵政銀行證書核證登記機關清單

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、暫時吊銷或撤銷及公佈銀行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。「1.3.6.1.4.1.16030.1.2.1」為本準則的物件識別碼 (Object Identifier, OID) (見附錄 B 內關於核證政策(Certificate Policies)的說明)。

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)申請人身份之程序,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的銀行證書將得到倚據證書人士之倚據並用來核實數碼簽署。利用由香港郵政發出之證書之各倚據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份可信,可用來認證各倚據證書人士特定之公匙基建應用程序上之參與者身份。

根據條例,香港郵政為認可核證機關。而根據本核證作業準則而發出的銀行證書,香港郵政已指明為認可證書。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、暫時吊銷或撤銷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(包括銀行證書)。換言之,香港郵政指定為認可證書者(如銀行證書)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)。香港郵政已指定銀行證書核證登記機關為其代理人之事實並無減輕香港郵政使用穩當系統之義務,亦無變更銀行證書作為獲認可證書具有之特性。

附錄 D 載有銀行證書特點摘要。

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獲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 2.1.4 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 2.1.4 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

只要分包商同意與香港郵政簽定合約承擔有關職務,香港郵政可把履行本準則及登記人協議之部份或全部工作之義務,進一步批予分包商執行。無論有關職務是否批出予分包商執行,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,共有兩類最終實體:登記人及倚據證書人士。登記人指於附錄 A 內所指的“登記人”或“登記人機構”。倚據證書人士乃倚據香港郵政發出之任何類別或種類證書(包

括但不限於銀行證書)以用於交易之實體。特此澄清,倚據證書人士不應倚據核證登記機關。香港郵政透過其代理人核證登記機關發出銀行證書,而核證登記機關對倚據證書人士並無任何謹慎職責,亦不需對倚據證書人士就發出銀行證書而負責(見第 2.1.2 條)。倚據其他登記人之證書(包括銀行證書)以用於交易之申請人或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:銀行證書可能不會發予未成年人(見附錄 E)。

1.2.2.1 登記人之保證及陳述

各申請人(如申請銀行證書(機構),獲授權代表會代表登記人機構)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) 除登記人及銀行證書(機構)之獲授權用戶外,並無其他人士曾取用登記人之私人密碼匙。
- b) 使用與登記人銀行證書所載之公開密碼匙相關之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、商用名稱、公司名稱或任何知識產權。
- f) 銀行證書(機構)只會由授權用戶用於授權應用中,請參閱以下第 1.2.3.2 條。

1.2.3 登記人之級別

根據本準則香港郵政僅發出證書予其申請已獲批准並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,香港郵政會發出兩類銀行證書,但各核證登記機關可決定及與香港郵政同意其是否接受兩類申請並於證書內予以識別或僅接受一類,如為一類,則屬那一類。

就銀行證書(機構)而言,根據本準則之規定,只有登記人機構須成為登記人。

1.2.3.1 銀行證書(個人)

銀行證書(個人)發給持有香港身份證及十八歲或以上人士。此等證書可用來從事商業用途。

1.2.3.2 銀行證書(機構)

銀行證書(機構)發給獲香港特別行政區政府簽發有效商業登記證之機構及獲香港法例認可之本港法定團體(即“登記人機構”),並識別已獲該登記人機構授權使用該銀行證書(機構)之私人密碼匙之成員或僱員(即“獲授權用戶”)。

經由核證登記機關發出之銀行證書(機構)只會由獲授權用戶用於附錄 E 中相對該核證登記機關之服務或系(“獲授權應用”)。

1.2.4 證書之期限

根據本核證作業準則發出之證書可能有不同期限,取決於核證登記機關就各證書之規定。香港郵政將就核證登記機關規定之證書期限與核證登記機關達成一致意見。證書之期限載於附錄 E (證書續期見第 3.2 條)。

1.2.5 在香港郵政批核之處所進行申請

所有首次申請及於證書撤銷或到期後之申請,申請人須依據第 3 及 4 條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、暫時吊銷或撤銷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訂定金錢限額。

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、暫時吊銷或撤銷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) 通知登記人有關已批准或被拒絕的申請（見第 4.1 條）；
- c) 通知登記人有關已批准的申請及如何提取證書（見第 4.2 及 4.3 條）；
- d) 暫時吊銷或撤銷證書及依時公佈證書撤銷清單（見第 4.4 條）；及
- e) 通知登記人有關已暫時吊銷或撤銷的證書（見第 4.4.1, 4.4.2 及 4.4.3 條）；

2.1.2 核證登記機關之義務及責任

核證登記機關僅遵照與香港郵政就獲其指定為代理人，代表其履行本準則詳述之若干義務而訂立之合約（代理人合約）之條款對香港郵政負責。核證登記機關代表香港郵政收集及保留根據本準則及登記人協議之條款所提供之文件及資料。香港郵政須由始至終對其核證登記機關所執行或其本意是執行香港郵政的功能、權力、權利和職責負責。

核證登記機關不為任何登記人協議之簽約方，亦不就發出、暫時吊銷、撤銷或公佈銀行證書，或就收集及保留文件或資料對登記人或倚據證書人士承擔任何謹慎職責。核證登記機關之行為僅為履行香港郵政於此事項之義務及責任。核證登記機關有權代表香港郵政實施登記人協議之條款（除非及直至該機關被撤銷及登記人正式獲通知任何該等撤銷）。**在任何情況下，核證登記機關不須就登記人協議或核證登記機關代表香港郵政作為認可核證機關發出之證書對登記人或倚據證書人士承擔任何責任。**

2.1.3 登記人之義務

登記人負責：

- a) 同意香港郵政，在其處所內使用穩當的系統，在安全的環境下代表登記人製作配對密碼匙。
- 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（如申請銀行證書（機構），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) 承認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、泄露或未經授權使用之義務。

- d) 發現其私人密碼匙之任何丟失或外泄時，立即向相關證書中指明之核證登記機關呈報丟失或外泄（外泄乃屬違反保安，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）。
- e) 不時將登記人提供之證書資料之任何變動立即通知予相關證書中指明之核證登記機關。
- f) 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相關證書中指明之核證登記機關。
- g) 同意其透過獲發出或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。
- h) 在登記人明知香港郵政或相關證書中指明之代表香港郵政之核證登記機關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核證登記機關知會，核證登記機關（代表香港郵政行事）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。
- i) 在明知核證登記機關可能據以撤銷證書之任何事項之情況下，或如上文 g) 所述登記人作出撤銷申請或經核證登記機關知會擬撤銷證書時，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，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。
- j) 就銀行證書（機構）而言，只適用於授權應用中。

2.1.3.1 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。

2.1.4 倚據證書人士之義務

倚據銀行證書之倚據證書人士負責：

- a) 倚據證書人士於倚據證書時如考慮過所有因素後仍確信倚據證書實屬合理之舉，方可倚據證書。
- 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，而核證登記機關（見附錄 E）並不對倚據證書人士承擔任何謹慎職責。
- c) 於倚據證書前查核證書撤銷清單上之證書狀態。
- d) 履行所有適當之證書核實程序。

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 合理技能及謹慎

香港郵政向各登記人及各倚據證書人士承諾，根據本準則香港郵政或代表香港郵政之核證登記機關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。香港郵政不保證其本身或核證登記機關或其他任何一方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，儘管香港郵政或代表香港郵政之核證登記機關於執行本合約及行使及履行其根據本準則之權利及義務時採取合理程度之技術及謹慎，若登記人作為本準則定義下之登記人或倚據證書人士或非登記人作為倚據證書人士遭受出自本準則中描述之公開密碼匙基建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，各登記人同意及各倚據證書人士須承認香港郵政、香港郵政署及任何核證登記機關概無需承擔任何責任、損失或損害。

即如在香港郵政或代表香港郵政之核證登記機關已採取合理程度之技術及謹慎之前提下，若登記人或倚據證書人士因倚據另一登記人由香港郵政所發出之銀行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、香港郵政署及任何該等核證登記機關概不負責。

亦即如在香港郵政（香港郵政署或代表香港郵政之核證登記機關）已採取合理程度之技術或謹慎以避免及/或減輕無法控制事件後果之前提下，若登記人或倚據證書人士因香港郵政不能控制之情況下遭受不良影響，香港郵政、香港郵政署或任何該等核證登記機關概不負責。香港郵政控制以外之情況包括但不限於互聯網或電訊或其他基建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，登記人僅有權促使證書發出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作出供應商品的陳述或保證。香港郵政雖同意將上述物品轉讓予登記人作本核證作業準則之指定用途，但亦承諾合理謹慎確保此等物品適合作本核證作業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，由香港郵政轉讓的物品可內載其他與完成及接受銀行證書無關之資料。若確實如此，與此等資料有關之法律觀點並非由核證作業準則或登記人協議規管，而須由物品內另行載述之條款決定。

2.2.3 法律責任限制

2.2.3.1 限制之合理性

各登記人或倚據證書人士必須同意，香港郵政按登記人協議及本準則所列之條件限制，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) 登記人協議；或
- b) 任何謹慎職責——尤其就登記人或倚據證書人士而言，當登記人、或倚據證書人士或其他人以任何方式倚據香港郵政根據此公開密碼匙基建發出或被代為發出之任何證書時，根據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

之情況下，登記人或倚據證書人士（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）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、失去工程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——200,000 港元

除下文所述之例外情況外，在香港郵政違反：

- a) 登記人協議；或
- b) 任何謹慎職責，尤其就登記人或倚據證書人士而言，當登記人或倚據證書人士或其他人士以任何方式倚據香港郵政根據此公開密碼匙基建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份）所負法律責任限制於任何情

況下，就每份銀行證書（個人）或每份銀行證書（機構）而言，不超過 200,000 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欲向香港郵政提出索償，且該索償源於或以任何方式與發出、暫時吊銷、撤銷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、核證登記機關及其各自之人員

無論香港郵政署或任何核證登記機關或其各自之任何職員、僱員或其他代理人均非登記人協議之簽約人，登記人及倚據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，香港郵政或任何核證登記機關或其各自之任何職員、僱員或代理人均不會自願接受或均不會接受向登記人或倚據證書人士擔負其任何個人出於真誠以任何方式與香港郵政履行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之任何行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份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、個人傷害或死亡之責任

任何因欺詐或蓄意之不當行為、個人傷害或死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

香港郵政發出之銀行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認可核證機關發出本證書。

因此，任何人士倚據本證書前均應閱讀適用於銀行證書之核證作業準則，可瀏覽香港郵政之網址 <http://www.hongkongpost.gov.hk>，或前往該證書中指明之代表香港郵政之核證登記機關處所及瀏覽其網址（見附錄 E）。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、僱員及代理人包括但不限於核證登記機關）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. 履行所有適當證書路徑認可程序。

若儘管香港郵政署長、香港郵政署、本證書中指明之任何核證登記機關及其各自之職員、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、本證書中指明之任何核證登記機關及其各自之職員、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、本證書中指明之任何核證登記機關、其各自之職員、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 200,000 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，香港郵政已獲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 200,000 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、本證書中指明之核證登記機關及其各自之任何職員、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。

提出索賠時間限制

任何倚據證書人士如擬向香港郵政署長索賠，且該索賠源起於或以任何方式與發出、暫時吊銷、撤銷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、本證書中指明之任何核證登記機關及其各自之職員、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證書所承擔之責任

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，因銀行證書（個人）或銀行證書（機構）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，登記人須將此情況立即通知證書中指明之核證登記機關，以便撤銷證書及（如願意接受）重新發出。登記人須即時通知有關核證登記機關，以撤銷證書及（如願意接受）重新發出。若登記人於接受證書後三個月內發出通知，且不再需要證書，而代表香港郵政之有關核證登記機關同意確有此差錯，有關費用將會退還。若登記人於接受證書三個月過後方將任何此類差錯通知有關核證登記機關，則費用將不會退還，而僅可由代表香港郵政之有關核證登記機關酌情退回。

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

除非獲得香港郵政授權，核證登記機關、香港郵政署或任何核證登記機關之代理人或僱員均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

倘本準則與登記人協議或其他規則、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

香港郵政或代表香港郵政之任何核證登記機關在任何時候均非登記人或倚據證書人士之代理人、受信人、受托人或其他代表。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或代表香港郵政之任何核證登記機關承擔登記人或倚據證書人士之代理人、受信人、受托人或其他代表之責任。

2.2.11 交相核證

香港郵政在所有情形下均保留與另一家核證機關定義及確定適當理由進行交相核證之權利。

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區圍制。

2.3.2 可分割性、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。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，則以英文本為準。

2.4 收費

銀行證書之收費詳情載於**附錄 E** 相關核證登記機關一節。

2.5 公開發表資料及儲存庫

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有關銀行證書之其他資料。除每周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。香港郵政每次處理已批核之銀行證書申請後，即時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下述 URL 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

須根據電子交易條例(香港法例第 553 章)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、暫時吊銷或撤銷及公佈證書之系統是否妥善遵守本準則。

2.7 機密性

在履行與香港郵政發出、暫時吊銷或撤銷及公佈證書之有關任務時可取閱任何紀錄、書刊、紀錄冊、登記冊、通訊、資訊、文件或其他物料之香港郵政、核證登記機關及任何香港郵政分包商之人員，不得向他人披露該等紀錄、書刊、紀錄冊、登記冊、通訊、資訊、文件或物料，也不得允許或容受向他人披露該等紀錄、書刊、紀錄冊、登記冊、通訊、資訊、文件或物料。香港郵政會確保香港郵政、核證登記機關及任何香港郵政分包商之人員均會依循此條限制事項。作為根據本準則申請銀行證書之組成部份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佈。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。

3. 鑑別及認證

3.1 首次申請

銀行證書(個人)之申請人須親身到核證登記機關之處所或香港郵政指定機構之處所，並出示第 3.1.9 條所述之身份證明。

銀行證書(機構)之申請人，其獲授權代表須親身到指定之香港郵政處所或其他香港郵政指定之機構處所，並出示第 3.1.8 條所述身分證明。在銀行證書(機構)上列明之獲授權用戶，則無須親身遞交申請。

所有銀行證書申請人必須向申請表中指明之核證登記機關呈交一份填妥並經簽署之申請表。銀行證書(機構)之申請表亦須經申請人所屬登記人機構獲授權代表填妥及簽署，而登記人機構亦會成為登記人。申請獲申請表中指明之代表香港郵政之核證登記機關承認後，香港郵政即準備銀行證書並向申請人直接發出通知，或按登記人之選擇由申請表中指明之核證登記機關通知，說明如何發出及接受證書。

3.1.1 名稱類型

3.1.1.1 銀行證書(個人)

- a) 透過證書上的主體名稱（於附錄 B 內指明），包括登記人香港身份證上顯示之姓名，可識別銀行證書（個人）登記人之身份。登記人香港身份證號碼則以雜湊數值形式儲存於證書內（見附錄 B）。

3.1.1.2 銀行證書（機構）

透過證書上的主體名稱可識別銀行證書（機構）登記人機構之身份，該名稱由以下資料組成：

- 獲授權用戶香港身份證/護照上顯示之姓名；
- 登記人機構在有關香港政府部門或登記機關之登記名稱；及
- 登記人機構之香港公司註冊/商業登記號碼。

3.1.1.3 獲授權代表

登記人機構獲授權代表雖替登記人機構辦理銀行證書（機構）申請手續，但該人士不會於之銀行證書（機構）中得到識別。

3.1.1.4 機構中文名稱

銀行證書一律只用英文發出。只有中文名稱或只提供中文名稱作登記之機構，其名稱不會顯示在銀行證書上。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

所採用名稱之詞義必須為一般人所理解，方便辨識登記人身份。

3.1.3 詮釋各個名稱規則

該數碼證書會載入之登記人名稱（主體名稱）類型見第 3.1.1 條。有關銀行證書主題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（於附錄 B 內指明）應無歧義而具獨特性。然而，此準則不要求名稱某一特別部份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

香港郵政或代表香港郵政之核證登記機關對有關名稱爭議之事宜的決定為酌情性及最終決定。

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）並向核證登記機關及倚據證書人士申述，申請銀行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、公司名稱或任何其他知識產權。

3.1.7 證明擁有私人密碼匙之方法

登記人將擁有經由香港郵政代製密碼匙服務產生之私人密碼匙。利用代製密碼匙服務，香港郵政將在其處所內使用穩當的系統，在安全的環境下代登記人產生配對密碼匙及製作證書，以保證私人密碼匙不被干擾。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。所有登記人承認其須對銀行證書內與公開密碼匙相關之私人密碼匙負上保安責任。

3.1.8 機構申請人身份認證

銀行證書（機構）之申請，應由申請人之獲授權代表親身到指定之香港郵政處所或其他香港郵政指定之機構處所遞交，獲授權代表亦須出示其香港特區身份證或護照。每份銀行證書（機構）之

申請須附有以下文件：

- a) 蓋上申請機構 “For and on behalf of” (代表機構簽署) 印章及附有該機構的獲授權簽署之授權書。授權書註明該機構已授權有關人士 (即「獲授權代表」) 代表該機構提交申請及識別列於銀行證書 (機構) 上的獲授權用戶；
- b) 所有按此方式識別身分之獲授權用戶之香港身份證或護照副本；及
- c) 由有關香港登記機關發出證明此機構確實存在之文件。

3.1.9 個人申請人身份認證

各個銀行證書 (個人) 申請人身份之確認將透過如下運作完成：

各證書申請人須親身到核證登記機關之處所，出示填妥並已簽署之銀行證書申請表以及申請人之香港身份證。該前述處所人員將覆核並認證所有申請文件，隨後將申請遞交香港郵政核證機關處理。

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。香港郵政或核證登記機關均不會為過期、已吊銷或已撤銷之證書續期。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 銀行證書 (個人)

每一份銀行證書 (個人) 續期可無須如首次申請時般進行面對面認證登記人身份之程序。然而，一經續期，必須運用香港郵政之代製密碼匙服務產生新的配對密碼匙。登記人與香港郵政就產生此等新密碼匙之責任與上文所述產生原密碼匙之責任相同。於辦理續期手續時，登記人須向核證登記機關遞交一份已填妥及簽署之證書續期表格，並繳足應繳費用。證書續期表格可於核證登記機關網址 (見附錄 E) 下載，或於核證登記機關辦事處索取。於辦理續期手續時，原登記人協議中的條款將仍適用於已續期之證書，除非有條款與當時之核證作業準則中的條款發生衝突。倘若確實發生該等衝突，則須以核證作業準則中的條款為準。申請續期之申請人應於遞交續期表格前先細閱申請續期當日適用之核證作業準則中的條款。

3.2.2 銀行證書 (機構)

銀行證書 (機構) 不會自動續期。若香港郵政接收到續期申請，即會根據第 3.1.8 條所述「機構申請人身份認證」之過程重新進行認證。

3.2.3 已續期銀行證書之有效期

因應香港郵政的酌情權，發出給登記人的新銀行證書可由新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 (適用於銀行證書 (個人))、或到期日的一年後 (適用於銀行證書 (機構)) 屆滿。由此，新的銀行證書 (個人) 的有效期可超過三年，但不會超過三年另一個月。新的銀行證書 (機構) 的有效期可超過一年，但不會超過一年另一個月。

4 運作要求

4.1 證書申請

4.1.1 按本準則申請銀行證書之申請人必須填妥香港郵政與核證登記機關共同編定之表格，並須到核證登記機關處所、指定之香港郵政處所或其他香港郵政指定之機構處所遞交申請。

4.1.2 有關用以確定申請人身份所需文件，可參閱本準則第 3.1.8 條 (機構申請人身份認證)

及第 3.1.9 條（個人申請人身份認證）。在核證登記機關代表香港郵政完成核對身份手續後，各銀行證書「個人密碼信封」會以安全方式送遞給申請人或獲授權代表（適用於銀行證書（機構）申請）。

4.1.3 核證登記機關會通知申請人申請已獲批核，並可能列印由登記人提供之所有資料及要求登記人確認該等資料之準確性及真實性。若香港郵政 / 核證登記機關未能根據本準則列明的要求成功核實有關申請，香港郵政 / 核證登記機關會拒絕有關申請並通知申請人。核證登記機關與香港郵政經電子方式傳送之所有申請資料須使用由香港郵政訂明之規約。

4.2 發出證書

4.2.1 香港郵政進行產生配對密碼匙及製作證書的工序。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。

4.2.2 以密碼保護的私人密碼匙及證書將隨後被存儲在軟碟或替代存儲介質上。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；並以安全方式交付予申請人。

4.2.3 申請人同意，他們一旦接獲磁片或替代存儲介質，即須完全為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。

4.2.4 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。在完成送遞銀行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。

4.3 接受及公佈證書

4.3.1 香港郵政會為申請人提供合理機會，核對其銀行證書內容及確認接受其銀行證書。申請人可將填妥的接受證書表格以傳真、信件或電郵，或經指定網頁（www.hongkongpost.gov.hk）交回香港郵政，以確認接受銀行證書。

4.3.2 申請人亦可確認不接受其銀行證書及而香港郵政會撤銷該銀行證書。

4.3.3 在申請人確認接受其銀行證書後，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銀行證書（見第 2.5 條）。未獲接受的銀行證書不會於香港郵政的儲存庫公佈。

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要求撤銷倚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銀行證書公開密碼匙相關私人密碼匙之媒介，若已外泄或懷疑已外泄，各登記人必須立即按照本準則的撤銷程序，直接向香港郵政或證書中所指明之核證登記機關申請撤銷證書（見第 2.1.3(e)條）。

不論何時，若有以下情況，香港郵政及證書中所指明之代表香港郵政之核證登記機關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) 知悉或有理由懷疑登記人之私人密碼匙已外泄；
- b) 知悉或有理由懷疑證書上任何細節乃不真實或已變得不真實或證書由於其他原因不可靠；
- c) 認為證書並未根據準則妥當發出；
- 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) 任何適用於該證書之規例或法例有此規定；
- f) 認為登記人未曾繳付登記費；
- g) 知悉或有理由相信其出現在證書上之銀行證書（個人）登記人：
 - i) 死亡或已死亡；或
 - 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新協議或債務償還安排或自願安排；
 - 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。
- h) 知道或有理由相信其出現在銀行證書（機構）上指明之獲授權用戶已非登記人機構之成員或僱員；或
- i) 知道或有理由相信其資料出現在銀行證書（機構）上之登記人：
 - i) 正被清盤或接到有司法管轄權之法庭所判清盤令；
 - ii) 在擬撤銷證書前五年內已達成香港法例第六章破產條例所指之債務重新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、舞弊或不誠實行爲，或違反電子交易條例被定罪；
 - iv) 在撤銷證書前五年內登記人資產之任何部份託給接管人或管理人接管。

4.4.2 撤銷程序請求

登記人，或登記人機構的獲授權代表，可直接透過傳真、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。登記人亦可透過傳真、郵寄信件、電子郵件或親身前往核證登記機關式視乎何種方式可為所聯繫機關接納而定，向證書中指明之核證登記機關提出撤銷要求（見附錄 E）；而該核證登記機關會將撤銷證書要求轉遞給香港郵政。

香港郵政接到此要求後會暫時吊銷證書。經登記人，或經初始接收撤銷證書要求的核證登記機關，最後確認撤銷證書後，該證書即會撤銷且永久失效。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為有效。但香港郵政只會在謹慎的情況下把暫時吊銷的證書回復為有效。

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“暫時吊銷”狀態回復有效的證書。

證書中所指明之核證登記機關（香港郵政之代理人）會在收到撤銷申請或相關撤銷證書之最後確認程序後，一個工作日內通知香港郵政，以便其將吊銷或撤銷之證書相應地刊載於證書撤銷清單內。

倘若核證登記機關在某一個非工作日之前一天收到撤銷申請或撤銷證書之最後確認證書，核證登記機關將立即通知登記人，彼等須將其撤銷申請或最後確認書直接送往香港郵政。

核證登記機關及香港郵政只能在正常辦公時間內處理撤銷申請或及撤銷證書之最後確認程序。核

證登記機關辦理撤銷證書事務之辦公時間詳情請參照附錄 E。

香港郵政處理撤銷證書要求的辦公時間如下：

星期一至星期五	：上午九時至下午五時
星期六	：上午九時至中午十二時
星期日及公眾假期	：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，香港郵政將停止處理撤銷證書要求。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（1）於直接從登記人收到或從證書中所指明之核證登記機關處收到撤銷申請或撤銷證書之最後確認書時或（2）在無此申請之情況下，香港郵政及/或代表香港郵政之核證登記機關決定暫時吊銷或撤銷證書時，確保在兩個工作日內，將該暫時吊銷或撤銷證書於證書撤銷清單公佈。然而，證書撤銷清單並不會於各證書暫時吊銷或撤銷後隨即公佈。而只會在下一份證書撤銷清單更新並公佈時，才會反映該證書已被撤銷之狀態。證書撤銷清單每日均會公佈，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，一律不視作第 4.4.3（a）條所述目的之工作日計算。

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/或證書中所指明之核證登記機關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或代表香港郵政之核證登記機關，香港郵政或代表香港郵政之核證登記機關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，則香港郵政及核證登記機關毋須就任何該等交易向登記人或倚據證書人士承擔責任。
- c) 此外，登記人明知香港郵政及/或證書中所指明之核證登記機關可能撤銷證書之任何事項之情況下，或登記人作出申請或經知會香港郵政或核證登記機關擬撤銷證書時，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、核證登記機關或經登記人申請），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，則香港郵政及核證登記機關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。

除非香港郵政或代表香港郵政之核證登記機關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撤銷證書人士，否則，香港郵政及核證登記機關無須就香港郵政及核證登記機關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與證書撤銷清單之內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份規限之範疇。在任何情況下，核證登記機關自身無須對倚據證書人士承擔獨立 謹慎責任（核證登記機關只是履行香港郵政之謹慎責任）。因此，即使出現疏忽，核證登記機關亦無須對倚據證書人士負責。

- d) 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暫時吊銷或撤銷的證書的資料時的政策，已列於本準則第 2.1.4 條(倚據證書人士之義務)及第 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後，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

香港郵政核證機關係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份的過程
- 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
 - 彙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 處理記錄次數

香港郵政每日均會處理及覆檢審核運行記錄，用以審核追蹤有關供香港郵政核證機關的行動、交易及程序。

4.5.3 審核記錄之存留期間

存檔審核記錄文檔存留期為七年。

4.5.4 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。

4.5.5 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）為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。

4.5.6 審核資料收集系統

香港郵政核證機關係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 記錄存檔

4.6.1 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：

- 系統設備結構檔案
- 評估結果及／或設備合格複檢(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
- 定期事件記錄
- 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

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為期不超過二十年。香港郵政核證機關密碼匙及證書在期滿前至少三個月會進行續期。續發新根源密碼匙後，相連之根源證書即會公佈供大眾取用。原先之根源密碼匙則保留至第 4.6.2 條指定之最短之時限，以供核對用原先密碼匙進行產生之簽署。

4.8 災難復原及密碼匙資料外泄計劃

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
- b) 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 處理密碼匙資料外泄計劃

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

如根據本準則用作發出香港郵政銀行證書的香港郵政私人密碼匙資料外泄，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泄，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銀行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。

4.10 核證登記機關終止服務

如核證登記機關停止擔任核證登記機關之職能，且其代表香港郵政行使之授權已予以收回，香港郵政或相應核證登記機關將知會指明該核證登記機關之證書之登記人。儘管核證登記機關進一步代表香港郵政之權力被終止，銀行證書仍按其條款繼續有效直至屆滿（惟登記人必須就先前由核證登記機關處理與銀行證書有關之事項直接與香港郵政交涉者除外），且於屆滿時，前核證登記機關須認可銀行證書繼續有效。倘代表香港郵政之核證登記機關之權力被撤回，則指明該核證登記機關之銀行證書於屆滿後不得續期。

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，為核證機關運作做好準備。

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

媒體存儲及處理程序已經開發備妥。

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 4.8.1.1 條)。

5.1.8 保管印刷文件

印刷文件包括登記人協議及身份確認文件之影印本由香港郵政或其核證登記機關妥為保存。獲授權人員方可以取閱該等記錄。

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，以及代表香港郵政行使權利之核證登記機關之僱員、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、彙編及推行相關程序。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

5.2.2 港郵政與核證登記機關之間的文件及資料傳遞

香港郵政與核證登記機關之間的所有文件及資料的傳遞，均在受控制及安全的方式進行。

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 2.6 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，以及代表香港郵政行使權利之核證登記機關人員，包括其僱員、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

香港郵政調查及／或要求核證登記機關調查其擔任受信職責之人員(其受聘前及其後按需要定期進行)，以按本準則之規定核實僱員之可信度及是否適任。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

香港郵政人員及核證登記機關人員已接受履行其職責所需要之初步培訓。有需要時香港郵政及核證登記機關亦會提供持續培訓，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

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

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能措施。控制香港郵政核證機關密碼匙之工作透過實體保安及穩妥密碼匙存儲進行。產生、儲存、使用及毀滅香港郵政核證機關密碼匙只能在由多人式控制之可防止篡改硬件裝置內進行。

6.1 產生及安裝配對密碼匙

6.1.1 產生配對密碼匙

除非程序被獲授權用戶外泄，否則香港郵政及申請人/登記人配對密碼匙之產生程序可使配對密碼匙的獲授權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。倘若由香港郵政為申請人代製密碼匙，在完成送遞銀行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銀行證書（個人）及銀行證書（機構）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址 <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

香港郵政銀行證書（個人）及香港郵政銀行證書（機構）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 FIPS140-1 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 級保安標準的裝置加密及儲存。香港郵政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二十年。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，控制活動數據（如個人辨識密碼及接達核證機關系統密碼的生命周期）。香港郵政已製定保安程序，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泄等情況。此等保安控制措施接受第 2.6 條遵守規定之評估。

6.5 生命周期技術保安控制

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 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份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 載有銀行證書之特點摘要。

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址 <http://www.hongkongpost.gov.hk> 或香港郵政儲存庫公佈，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。就任何對本準則作出的更改，香港郵政會實際可行地儘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址 <http://www.hongkongpost.gov.hk> 或有關核證登記機關網址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」指申請銀行證書之自然人或法人。

「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。

「授權應用」指核證登記機關發出之銀行證書可能只適用於附錄 E 第五欄中相對該核證登記機關之服務或系。

「獲授權代表」指登記人機構之授權代表。

「獲授權用戶」指登記人機構之成員或僱員；而登記人機構已授權該成員或僱員使用發出予該登記人機構的銀行證書（機構）的私人密碼匙。

「證書」或「銀行證書」指符合以下所有說明之記錄：

- (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份或其他主要特徵；
- (b) 識別發出記錄之核證機關；
- (c) 指名或識別獲發給記錄者；
- (d) 經發出記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佈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」就電子記錄而言，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記錄作數據變換產生，使持有原本未經數據變換之電子記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，原本之電子記錄是否未經變更。

「電子記錄」指資訊系統產生之數碼形式之記錄，而該記錄：

- (a) 能在資訊系統內傳送或由一個資訊系統傳送到另一個資訊系統；並
- (b) 能儲存在資訊系統或其他媒介內。

「電子簽署」指與電子記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記錄之目的訂立或採用者。

「身份證」指由香港特別行政區政府入境事務處發出的香港身份證，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) 記錄資訊；

- (c) 用作使資訊記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（不論該等資訊記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**」就某特定電子記錄而言，指代他人發出、接收或儲存該記錄，或就該記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。

「**線上即時認證**」指經由互聯網確認證書有效性之協定。

「**條例**」指香港法例第 553 章電子交易條例。

「**發訊者**」就某電子記錄而言，指發出或產生記錄者，或由他人代為發出或產生該記錄者，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。

「**記錄**」指在有形媒界上註記、儲存或以其他方式固定之資訊，亦指儲存在電子或其他媒界可藉理解形式還原之資訊。

「**核證登記機關**」指由香港郵政指定，代表香港郵政行使一定職能，並提供香港郵政之若干服務之機構。

「**倚據限額**」指就認可證書倚據而指明之金額限額。

「**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記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**」指符合以下所有說明的人：

- (i) 在某證書內指名或識別為獲發給證書；
- (ii) 已接受該證書；或
- (iii) 持有與列於該證書內的公開密碼匙對應之私人密碼匙；

「登記人協議」指由登記人及香港郵政訂立的協議，包含在申請表上列明的登記人條款及條件及本核證作業準則的條款。

「登記人機構」指作為登記人的機構；而其獲授權代表已簽署登記人協議及根據此核證作業準則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件、軟件及程序：

- (a) 合理地安全可免遭受入侵及不當使用；
- (b) 在可供使用情況、可靠性及操作方式能於合理期內維持正確等方面達到合理水平。
- (c) 合理地適合執行其原定功能；及
- (d) 依循廣為接受之安全原則。

為執行電子交易條例，如某數碼簽署可參照列於某證書內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 - 香港郵政銀行證書格式

1) 銀行證書 (個人) 格式

欄位名稱	欄位內容	
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
發行者名稱 (Issuer Name)		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 Bank-Cert (XXX- Personal) (附註4) c=HK
主體公開密碼匙資料 (Subject public key info)		算式識別 (Algorithm ID) : RSA 公開密碼匙 (Public key) : 密碼匙長度為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)	發行者 (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 (此欄為"關鍵"欄位)
證書政策 (Certificate policy)		PolicyIdentifier = 1.3.6.1.4.1.16030.1.2.1 (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)
	第一目錄名稱的共同名稱 (1 st Directory Name CN)	[核證登記機關參考資料]
發行者其他名稱 (Issuer alternative name)		未使用
基本限制 (Basic)	主體類型	最終實體

欄位名稱		欄位內容
constraints)	(Subject type)	
	路徑長度限制 (Path length constraints)	無
延伸密碼匙的使用 (Extended key usage)		未使用
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 (Netscape 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. XXX 為核證登記機關名稱 (見附錄 E)
5. 除非另外註明, 所有標準延伸欄位及 Netscape 延伸欄位均為 “非關鍵” (Non-Critical) 延伸欄位。
6. 香港郵政已獲 Internet Assigned Numbers Authority (IANA) 分配私人企業號碼 (Private Enterprise Number) 16030 號。「1.3.6.1.4.1.16030.1.2.1」為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為一雜湊數值(以 cert_hkid_hash 表示)後, 存入證書:

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

SHA-1 為一雜湊函數而 RSA 則為簽署函數

在代製密碼匙的過程中, hkid_number 則會在香港郵政處所內代製密碼時簽署, 並產生已簽署的香港身份證號碼的雜湊數值 $SHA-1 (RSA_{privatekey, sha-1} (hkid_number))$ 。該雜湊數值會輸入證書內的指定延伸欄位。

8. 證書撤銷清單分發點 URL 為 <http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL2.crl>。

2) 銀行證書 (機構) 格式

欄位名稱	欄位內容	
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
發行者名稱 (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=[獲授權用戶姓名] (附註1) e=[電子郵箱地址] (附註2) ou=[登記人參考編號] (附註3) ou=[商業登記證書編號+註冊證書/登記證書編號+其他] (附註4) ou=「登記人機構名稱」(附註5) ou=「登記人機構分行/部門名稱」 o=Hongkong Post Bank-Cert (XXX-Corporate) (附註6) 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7)		
機關密碼匙識別名稱 (Authority key identifier)	發行者 (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 (此欄為「關鍵」欄位)
證書政策 (Certificate policy)		PolicyIdentifier = 1.3.6.1.4.1.16030.1.2.1 (附註8) PolicyQualifierID = CPS Qualifier = [核證作業準則的URL]
主體其他名稱 (Subject alternative name)	DNS	未使用
	rfc822	[證書持有人電子郵箱地址] (附註2)
	第一目錄名稱的共同名稱 (1 st Directory Name CN)	[核證登記機關參考資料]
發行者其他名稱 (Issuer alternative name)		未使用
基本限制 (Basic constraints)	主體類型 (Subject type)	最終實體

欄位名稱		欄位內容
	路徑長度限制 (Path length constraints)	無
延伸密碼匙的使用 (Extended key usage)		未使用
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9)
Netscape 延伸欄位 (Netscape extension) (附註6)		
Netscape 證書類型 (Netscape 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. 獲授權用戶姓名格式: 英文格式 - 姓氏 (大寫) + 名 (例如 CHAN Tai Man David)
2. 獲授權用戶電子郵箱地址 (選項)
3. 登記人參考編號: 10 位數字
4. “商業登記證書編號”欄位: 16 位數字 (首 11 位數字代表商業登記編號), “註冊證書 / 登記證書編號”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。
5. 只有中文名稱或只提供中文名稱作登記之機構, 其名稱不會在此欄內顯示(見本核證作業準則第 3.1.1.4 條)。
6. XXX 為核證登記機關名稱 (見**附錄 E**)
7. 除非另外註明, 所有標準延伸欄位及 Netscape 延伸欄位均為 “非關鍵” (Non-Critical) 延伸欄位。
8. 香港郵政已獲 Internet Assigned Numbers Authority (IANA) 分配私人企業號碼 (Private Enterprise Number) 16030 號。「1.3.6.1.4.1.16030.1.2.1」為本準則的物件識別碼 (Object Identifier, OID)。
9. 證書撤銷清單分發點 URL 為 <http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL2.crl>

附錄C - 香港郵政證書撤銷清單(CRL)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] 時間 01:15、06:15 及 11:00））；證書撤銷清單載有根據本核證作業準則而暫時吊銷或撤銷的銀行證書的資訊：

- a) 「**分割式證書撤銷清單**」 (Partitioned CRL) 包含分組的已暫時吊銷或已撤銷證書的資料。公眾可於在證書的「證書撤銷清單分發點 (CRL distribution point)」欄位內註明的 URL 獲取相關的「分割式證書撤銷清單」。
- 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。公眾可於以下 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 \(port 389, cn=Hongkong Post e-Cert CA 1 CRL1, o=Hongkong Post, c=HK\)](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 條）。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 版本為 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
發行者 (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 (Revocation date)	[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欄位 (CRL entry extensions)			
	原因代碼 (Reason code)	[撤銷理由識別碼]		(附註 1)

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
標準延伸欄位 (Standard extension) (附註 2)				
機關密碼匙識別名稱 (Authority key identifier)	發行者 (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)] (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。

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 - 香港郵政銀行證書 — 服務摘要

服務	銀行證書（個人）	銀行證書（機構）
登記人	持有有效香港身份證及年滿 18 歲人仕	獲香港特別行政區政府簽發有效商業登記證之機構及獲香港法例認可之本港法定團體
證書持有人	即登記人	登記人機構之成員或僱員並為獲授權用戶
依據限額	HK\$200,000	HK\$200,000
認可證書	是	是
配對密碼匙	1024-bit RSA	1024-bit RSA
核證登記機關	見附錄 E	見附錄 E
製造配對密碼匙	由香港郵政代製	由香港郵政代製
核實身份	須核對登記人的身份	須核對機構及其獲授權代表的身份
證書的用途	數碼簽署及加密	數碼簽署及加密
證書內包含登記人的資料	<ul style="list-style-type: none"> ▪ 香港身份證上列出的英文姓名； ▪ 香港身份證號碼的雜湊數值 (hash value)； ▪ 電郵地址；及 ▪ 登記人參考編號（由香港郵政系統產生） 	<ul style="list-style-type: none"> ▪ 登記人機構名稱 ▪ 獲授權用戶英文姓名及其電郵地址 ▪ 登記人參考編號（由香港郵政系統產生） ▪ 登記人機構之公司 / 商業登記資訊
登記費用及證書有效期	見附錄 E	見附錄 E

附錄E - 香港郵政銀行證書核證登記機關名單

核證登記機關名稱 / 網址	證書名稱	證書有效期	未成年人可否登記	授權應用	撤銷證書辦公時間 / 撤銷證書辦法	登記費用
東亞銀行有限公司 / www.hkbea.com	香港郵政銀行證書(東亞銀行一機構)	一年	否	只適用於東亞銀行之企業電子網絡銀行服務及由ESD Services Limited 公佈之香港特別行政區政府「公共服務電子化」計劃內之服務。	星期一至星期五：上午九時至下午五時 星期六：上午九時至下午一時 星期日及公眾假期：除外 / 撤銷證書申請可透過郵寄信件或親身遞交。	首次登記：20港元 重新申請或續期：120港元
上海商業銀行有限公司 / www.shacombank.com.hk	香港郵政銀行證書(上海商業銀行一個人)	三年	否	適用於所有符合本準則條文之穩妥交易及其他商業營運。	星期一至星期五：上午九時至下午五時 星期六：上午九時至下午一時 星期日及公眾假期：除外 / 撤銷證書申請可透過郵寄信件、電話、電子郵件或親身遞交。	銀行證書(個人): 申請或續期：60港元
	香港郵政銀行證書(上海商業銀行一機構)	一年	否			銀行證書(機構): 首次登記：20港元 重新申請或續期：120港元