認可核證機關業務守則的修訂擬稿

引言

本文件旨在向《電子交易條例草案》審議委員會介紹認可核證機關業務守則（簡稱「業務守則」）的修訂擬稿。

背景

2. 根據《電子交易條例草案》第 27D 條規定，資訊科技署署長（簡稱「署長」）可發出業務守則，訂明認可核證機關在執行功能時所採用的標準及程序。資訊科技署已於本年十月二十五日公布業務守則的初稿，並進行公眾諮詢，直至十一月十五日爲止。資訊科技署共接獲下列八間機構和一位市民的書面意見–

- 英國電腦學會〔香港分會〕；
- 香港電訊；
- 消費者委員會；
- 香港大律師公會；
- 香港電腦學會；
- 香港工程師學會〔資訊科技組〕；
- 個人資料私隱專員公署；
- 貿易通電子貿易有限公司； 及
- 一位市民。

此外，資訊科技署亦曾就業務守則的擬稿，與其他機構（例如香港會計師公會等）商討和交換意見。

3. 在本年十一月二十九日舉行的《電子交易條例草案》審議委員會第八次會議上，我們向各議員簡介就業務守則進行公眾諮詢所收到的主要意見以及我們的初步回應。

守則的修訂擬稿

4. 經考慮諮詢時所取得的意見及議員所提出的意見後，資訊科技

署已修訂業務守則擬稿，並大幅度豐富其內容。業務守則的修訂擬稿載於附件。主要修訂簡述如下 –

- 新增一項條文，規定如守則任何部分與經制訂的《電子交易條例》內的任何條文不符，則以條例內的有關條文爲準（修訂擬稿內第1.6段）；

- 增加條文，指明署長會在日後修訂業務守則時諮詢業界（修訂擬稿內第1.7段）；

- 就採用穩當系統提供詳細指引，包括一套獲廣泛認可的保安原則，及一套關於核證機關功能的最適當運作模式。兩者均是認可核證機關應予遵循的；以及

- 增加三個附件如下 -

- 附件一 ： 核證機關及證書的認可 - 該附件簡述核證機關及證書取得認可資格的準則及程序；

- 附件二 ： 認可核證機關的核證作業準則內容的指引；及

- 附件三 ： 核證機關遵守規定的評估 - 該附件列出擬備核證機關遵守規定的評估報告的人士的基本資歷，及評估報告所應涵蓋的範圍。

進一步的諮詢

5. 資訊科技署已把業務守則的修訂擬稿送交曾就初稿發表具體意見的機構，並與這些機構就修訂擬稿進行磋商。對於資訊科技署擬備業務守則的修訂擬稿時所採取的方向，所有資訊科技署曾與接觸的機構均表支持。此外，這些機構亦表示接納守則擬稿內所臚列的原則和架構，及認爲這些原則和架構是恰當的。假如這些機構就擬稿的細節內容有任何進一步的意見，將會在短時間內向資訊科技署提出。這些關乎細節內容的意見應不會影響業務守則的大體方向及在該文件內臚列的原則和架構。資訊科技署會在考慮有關意見後完成製訂業務守則。

資訊科技及廣播局
一九九九年十二月

認可核證機關

業務守則

(修訂擬稿)

香港特別行政區政府

目錄

附件一　核證機關及證書的認可

附件二　有關核證作業準則內容的指引

附件三　核證機關遵守規定的評估

1 引言

1.1 本業務守則是資訊科技署署長(下文簡稱「署長」)根據《電子交易條例》(下文簡稱「條例」)發出。

1.2 本業務守則就認可核證機關在執行其功能時所需遵守的標準及程序提供指引。本業務守則應與條例一併閱讀。

1.3 署長根據條例第 20 條對核證機關作出認可時，會考慮該核證機關是否有能力遵守本業務守則。

1.4 署長根據條例第 21 條對個別證書或某類型、類別或種類的證書作出認可時，會考慮該證書或該類型、類別或種類的證書是否或會否由認可核證機關按照本業務守則發出。

1.5 署長根據條例第 21、22、23 或 26 條暫時吊銷、撤銷或不續發認可給某核證機關，或由該核證機關已發出或將發出的個別證書或某類型、類別或種類證書所獲批的認可時(視屬何種情況而定)，可考慮認可核證機關未能遵守本業務守則的情況。

1.6 如本業務守則任何部分與條例內的任何條文不符，則以條例內的有關條文爲準。

1.7 署長會不時對本業務守則作出修訂，並會就修訂諮詢業界（包括按照條例第 20 及 28 條所認可的核證機關）的意見。

2 用語定義

2.1 本業務守則內有關用語的定義如下：

證書 指符合以下所有說明的紀錄：-

- 由核證機關爲證明數碼簽署的目的而發出，並且該數碼簽署的用意是確認持有某特定配對密碼匙的人的身分或其他主要特徵的；
- 識別發出紀錄的核證機關；
- 指名或識別獲發給紀錄的人；

- 包含該獲發給紀錄的人的公開密碼匙；並且

- 由發出紀錄的核證機關的負責人員簽署；

核證機關	指向他人(可以是另一核證機關)發出證書的人；
核證機關證書	指向核證機關發出的證書(可以是核證機關發給自己的證書，即是「自我簽署」的證書)，用以證明該核證機關所發出的證書；
核證機關披露記錄	就認可核證機關而言，指由署長備存而公眾可查閱的關乎該機關的聯機紀錄，該紀錄包含與本條例目的有關的關乎該機關的資訊；
證書政策	指一套訂明的規則，表明證書對特定群體及/或有共同保安要求的使用類別的適用性；
核證作業準則	指核證機關所發出的以指明其在發出證書時使用的作業實務及標準的準則；
證書撤銷清單	指由核證機關備存及公布的清單，列明其發出及已撤銷的證書；
數碼簽署	就電子紀錄而言，指簽署人的電子簽署，而該簽署是用非對稱密碼系統及雜湊函數將該電子紀錄作數據變換而產生的，使持有原本未經數據變換的電子紀錄及簽署人的公開密碼匙的人能據之確定 - 該數據變換是否用與簽署人的公開密碼匙對應的私人密碼匙產生的；及 - 在產生數據變換之後，該原本的電子紀錄是否未經變更；
適當人選	除其他有關的任何事宜以外，指

- 該人沒有在香港或其他地方被裁定犯任何罪行，而該項定罪必然包含該人曾有欺詐性、舞弊或不誠實的作爲的裁斷；

- 該人無被裁定犯本條例所訂的罪行；

- 如該人是個人，其不是未獲解除破產的破產人，亦沒有在申請日期之前五年內曾訂立《破產條例》(第 6 章)所指的債務重整協議、債務償還安排或自願安排；及

- 如該人是一間公司，其並非正在清盤當中，亦不是任何清盤令的標的、亦沒有接管人就該公司而獲委任，亦沒有在申請日期之前五年內曾訂立《破產條例》(第 6 章)所指的債務重整協議、債務償還安排或自願安排;

資訊系統　　指符合以下所有說明的系統

- 處理資訊的；

- 記錄資訊的；

- 能用作使資訊記錄或儲存在不論位於何處的其他資訊系統內，或能用作將資訊在該等系統內以其他方式處理的；及

- 能用作檢索資訊(不論該等資訊是記錄或儲存在該系統內或在不論位於何處的其他資訊系統內);

發出　　就證書而言，指核證機關製造證書並將該證書的內容通知該證書內指名或識別爲獲發給該證書的人的作爲;

配對密碼匙　　在非對稱密碼系統中，指私人密碼匙及其在數學上相關的公開密碼匙，而該公開密碼匙是能核實該私人密碼匙所產生

的數碼簽署的;

私人密碼匙	指配對密碼匙中用作產生數碼簽署的密碼匙;
公開密碼匙	指配對密碼匙中用作核實數碼簽署的密碼匙;
認可證書	指 - 根據條例第 21 條認可的證書； - 屬根據條例第 21 條認可的證書的類型、類別或種類的證書；或 - 條例第 28 條提述的核證機關所發出的指明爲認可證書的證書;
認可核證機關	指根據條例第 20 條認可的核證機關，或條例第 28 條提述的核證機關;
負責人員	就某核證機關而言，指在該機關與本條例有關的活動方面身居要職的人;
倚據限額	指就認可證書的倚據而指明的金錢限額;
儲存庫	指用作儲存及檢索證書及其他與證書有關的資訊的資訊系統;
登記人	指符合以下所有說明的人(該人可以是另一核證機關) - 在某證書內指名或識別爲獲發給證書； - 已接受該證書；及 - 持有與列於該證書內的公開密碼匙對應的私人密碼匙;
穩當系統	指符合以下所有條件的電腦硬件、軟件及程序 - 是合理地安全可免遭受入侵及不當使用的；

- 在可供使用情況、可靠性及操作方式能於合理期間內維持正確等方面達到合理水平；
- 合理地適合執行其原定功能；及
- 依循獲廣泛接受的安全原則。

3 認可核證機關的一般責任

3.1 認可核證機關必須遵守署長根據條例第 20 條作出認可時附加的條件。對核證機關及證書作出認可的條件及程序載於附件一。

3.2 認可核證機關可委任代理人或次承判商執行其部分或全部工作，但必須符合下列條件：

- 該代理人或次承判商應同樣有能力遵守本業務守則適用於其運作的部分；及
- 核證機關必須對其代理人或次承判商所作的與條例相關的活動負最終的責任。

3.3 認可核證機關在發出及管理證書時，不應對其登記人或倚據由認可核證機關發出的認可證書的人士造成不合理的風險。

3.4 認可核證機關必須向署長呈交其核證機關證書，以供署長在核證機關披露紀錄內公布。有關的披露紀錄在該核證機關終止其服務七年內，提供令一途徑，讓有需要核實由核證機關發出的認可證書的人士，取得該核證機關的證書。

3.5 根據本業務守則規定，認可核證機關需把資料及紀錄加以記錄、保存或存檔。除本業務守則另外註明外，核證機關必須記錄、保存或存檔這些資料或紀錄，爲期不少於七年。

3.6 認可核證機關須遵守有關個人資料私隱的所有適用條例。

4 核證作業準則

4.1 認可核證機關必須就其發出的各類型、類別或種類的認可證書，向公眾公布及備存一份或以上最新的核證作業準則。認可

核證機關可按照不同類型、類別或種類的認可證書公布不同的核證作業準則，或根據其所發出的所有認可證書公布一份綜合的核證作業準則。

4.2 認可核證機關需在核證作業準則內訂明該核證機關及其登記人及倚據其發出的證書的人士的法律責任，限制其法律責任的事項及義務和核證機關在其證書內設定倚據限額的含意。認可核證機關需透過以下方法使其登記人及倚據核證機關發出證書的人士注意到該等法律責任、限制其法律責任的事項、義務及含意：

- 在與登記人訂立的任何合約或協議內適當地獨立指明有關資料；及
- 以書面形式及電子形式，透過聯機及可供大眾查閱的媒介適當地使有關方面可獲得該等資訊。

4.3 認可核證機關需在其核證作業準則內，就其發出的各類型、類別或種類的認可證書的認可情況，提供最新的資料。

4.4 認可核證機關需促使其登記人及倚據其認可證書的人士注意使用及倚據其發出但未獲署長認可的證書的影響。

4.5 認可核證機關需促使其登記人注意，在核證機關發出予登記人及在核證機關儲存庫公布的認可證書內加入的登記人個人資料會成爲公開資料。有關的核證作業準則必須明確界定與該核證作業準則相關的認可證書的內容。

4.6 認可核證機關在公布核證作業準則後應向署長提交該準則的副本，並於切實可行範圍內盡快通知署長其後任何有關該準則的轉變。認可核證機關亦需記錄準則的所有轉變及每項轉變的生效日期。

4.7 如果認可核證機關按照證書政策所指定而發出某類型、類別或種類的認可證書，該證書政策可作爲這些證書的有關核證作業準則的參考，而有關的證書政策應當作爲核證作業準則的一部分。

4.8 認可核證機關應保存其核證作業準則每個版本的副本，並應同時列明每個版本的生效日期及停止生效日期（如適用）。保存核證作業準則副本時應考慮到保安、完整性及以後存取及檢查是否方便。

4.9 認可核證機關在發出某類型、類別或其他種類的認可證書時，需遵守就該類型、類別或其他種類的認可證書的核證作業準則。

4.10 認可核證機關必須確保其核證作業準則隨時在其聯網的儲存庫內可供公眾查閱。當核證作業準則有更改時，該儲存庫必須盡快更新。

4.11 有關核證作業準則內容的進一步指引，請參閱附件二。

5 穩當系統

5.1 認可核證機關在提供其服務時必須使用穩當系統。其中包括產生及管理其密碼匙，產生及管理登記人的密碼匙(如適用)，認可證書的發出、續期、暫時吊銷(如適用)或撤銷，就認可證書的發出、續期、暫時吊銷或撤銷發出通知，設置儲存庫，以及在儲存庫內公布認可證書及其他資料。

闡釋

5.2 「系統」一詞非單指電腦的硬件及軟件，亦指有關的支援程序，包括人手及自動的程序、保安安排及系統運作的標準。

5.3 一個「穩當系統」需充分確保它能一致、可信及可靠地執行其特定的功能。一套系統是否屬穩當系統，須視乎有關的核證機關能否證明該系統運作的機制、程序及運作環境均足以令系統執行其特定的功能。

5.4 量度穩當程度並無一套絕對的標準。穩當程度只能在一個特定的範圍下作出量度。「合理」須按照最終使用的目的，及考慮所有有關情況後才能評估是否合適和恰當。

指導原則

5.5 按照條例所採用的科技中立及盡量少加規管的方針，認可核證機關可自行選擇採用何種特定技術方案以支援其運作。

5.6 然而，在核證機關的高風險運作範圍內，如有關保密的功能，核證機關所採納的系統及程序應符合國際上廣泛被接納或認可的標準。此外，作爲最適當的運作模式方面，認可核證機關應對其潛在風險進行有系統的評估，並採取合適的對策，以控制、減輕及監察有關風險。

應考慮的特定範圍

5.7 在公開密碼匙基礎建設下運作的認可核證機關一般需採用複雜的硬件、軟件及密碼綜合組件。這些組件需有適當的政策及程序配合，以確保核證機關能在穩妥的環境下運作。

5.8 認可核證機關達致維持系統穩當的方法，視乎不同核證機關提供的特定服務、可使用的技術及所面對的商業情況而可能有所不同。不過，認可核證機關必須遵守以下最適當的運作模式。

獲廣泛認可的行業內最適當運作模式

5.9 認可核證機關需就其營運環境制訂正式的政策、程序及方式，其中包括但並不限於下列所討論的範圍：

獲廣泛認可的保安原則

5.9.1 認可核證機關必須根據獲廣泛認可的保安原則，就其運作維持及執行足夠及適當的保安控制。其中至少應包括下列事項：

- 資產分類及管理；
- 人事保安；
- 實體及環境保安；及
- 系統使用的管理。

資產的分類及管理

5.9.2 認可核證機關需把其資產按邏輯作出適當的分類，並爲其主要資產認定擁有人。核證機關需保存其資產最新及最齊全的清單，並制訂程序以保障其資產。

5.9.3 該核證機關必須把其存有的資料當爲其中一種資產，並根據業務運作的重要性爲該等資料分類。該核證機關須制訂合適的控制措施，以防止擅自存取或破壞資料的情況。

人事保安管理

5.9.4 認可核證機關應透過下列機制有效控制人事保安，其中包括但不限於：

- 根據其保安政策透過正式的職務描述以界定職能及責任；
- 根據其保安政策及程序對其員工進行核證檢查；

- 在僱用合約的正式條款及條件內加進保密或類似協議。

5.9.5 認可核證機關需爲其職員提供適當的培訓，以維持他們的技術水平，並確保能有效實施及遵守保安政策。培訓的內容可包括但不限於以下範圍，：

- 適當的技術培訓；
- 組織政策和程序；及
- 發生事故的應變程序及將問題提升的程序；

5.9.6 認可核證機關必須制訂適當的控制措施以監察其人員的表現，例如：

- 定期進行的工作表現評核；
- 正式的紀律程序；及
- 正式終止服務的程序。

實體及環境保安

5.9.7 認可核證機關需維持有效的實體及環境保安控制措施，其中包括但不限於：

- 認定及界定保安範圍，並採取適當的保安控制措施以維持該等範圍的安全；
- 爲核證機關的員工及探訪者進入該等範圍制訂正式的程序；
- 設立合適的保安及出入監察機制，並特別注意核證機關儲存其高保密性設備的範圍；
- 制訂恰當的監控機制，防止其設備受火災、水災、停電等環境因素及災患影響，並防止有人未經許可而擅自進入有關範圍；
- 制訂一般保安監控措施，例如清理辦公桌政策及對於核證機關所有設備、資料及其他資產的一般控制；及
- 確保維持其環境控制機制，並按時作出修改。

5.9.8 如果認可核證機關倚賴第三方提供的服務(如透過外發協議)，保護實體及環境保安的規定必須適當地在與該第三方供應商所訂立的正式服務標準協議中指明。

5.9.9 如果認可核證機關倚靠外在的建築物管理服務保護其周圍實體及環境，則應與該服務供應商訂立適當的正式服務標準協議。

系統使用的管理

5.9.10 認可核證機關需就其資訊系統包括應用系統的使用制訂及採取有效的控制措施及程序。這些控制措施及程序應配合受保護系統的敏感性及重要性，其中包括但不限於：

- 制訂業務規定以控制進入系統；
- 正式界定用者的責任；
- 界定正式程序以管理用者號碼及監察進入其系統的情況，其中包括：
  - 分配、修改及撤銷用者的進入權；及
  - 利用存檔記錄及類似方法監察嘗試進入系統的情況；
- 就進入網絡、操作系統及應用系統如防火牆，路由器制訂控制措施；
- 就進入及使用監察系統制訂程序及控制措施；
- 就流動電腦運算及電訊運作制訂程序及控制措施；
- 就擅自或非法使用軟件制訂程序及控制措施；及
- 就處理有關進入網絡、操作系統及應用系統的保安事故制訂程序。

操作管理

5.9.11 認可核證機關需就其日常運作制訂有效的控制措施及程序。操作政策及標準操作程序必須得到正式確定及記錄，其中包括但不限於：

- 清楚界定其操作人員的職務及責任；
- 定期監察系統容量的程序以監察系統的功能及找出阻礙運作的地方；

- 訂立適當的程序，以防止其電腦基本設施受有害程式侵擾，如電腦病毒等；
- 適當的系統及網絡管理程序，包括備存及存檔等日常程序；
- 就電子資訊及媒體的處理、分發、儲存及棄置設立適當的程序；及
- 就提出重大問題而訂立正式的將處理問題的層次提升的程序，以便跟進及解決有關問題。

電腦系統的發展及維修

5.9.12 認可核證機關需對其系統的發展及維修活動制訂有效的控制措施及程序，其中包括：

- 制訂適當的內部標準，確保無論由核證機關的人員或在外發工作的情況下由外間機構進行發展工作，均能維持一致性；
- 設立程序以確保分隔生產及發展的環境；
- 設立程序以確保區分操作及發展人員的職責；
- 就獲取其生產及發展環境儲存的資料及進入有關系統制訂控制措施；
- 控制變更操控程序，包括系統及/或數據的緊急變更；及
- 就有關妥善管理設備及服務的採購工作制訂程序。

業務運作的持續性

5.9.13 認可核證機關需發展及維持涵蓋其所有主要營運層面的業務持續運作計劃。

5.9.14 按時對該持續運作計劃進行測試，而計劃所牽涉的有關主要人員須參與。在可能範圍內，對這些測試需要作出獨立的觀察。

5.9.15 業務持續運作計劃應包括緊急應變機制，如處理核證機關本身用以簽署登記人證書的私人密碼匙外洩或懷疑外洩的情況，或核證機關的系統或其組成部分出現嚴重問題的情況。

保存適當事件紀錄

5.9.16 認可核證機關需保存完備的事件紀錄，其中包括保留有關發出及管理核證機關認可證書的活動的文件。

5.9.17 認可核證機關在爲這些事件紀錄存檔時需確保這些紀錄穩妥、完整及方便存取和檢查。核證機關亦需定期檢查事件紀錄，並就所發現的任何不正常情況採取行動。

5.9.18 認可核證機關需爲所有重大事件備存紀錄，其中包括但並不限於：

- 用以產生密碼匙的材料及設備的存取；
- 密碼匙及證書的產生、發出、分派、儲存、備份、暫時吊銷、撤銷、撤回、存檔、銷毀及其他的有關事項；
- 涉及保安的敏感事件，包括密碼匙資料外洩；及
- 加密設備的採購、安裝、使用、解除運作及棄用。

對符合規定的監察及保證

5.9.19 認可核證機關需訂立適當的控制措施，以確保能符合有關的法律、規例及技術要求，其中包括但不限於：

- 設定適當的機制以監察核證機關各層面的運作，並確保符合有關的規定；
- 確保其監察機制的功能已達到業界的現行標準；及
- 就其操作系統安排適當的查核。

核證機關功能特定的最適當運作模式

5.10 認可核證機關需就其特定的核證機關功能制訂正式及經審批的政策、程序及方式，其中包括但不限於下列各段的範圍。

核證作業準則的管理

5.10.1 認可核證機關需在其核證作業準則披露其業務常規，並對其核證作業準則作出有效控制，其中包括但不限於：

- 設立管理小組，並授予訂定及審批核證作業準則的權力及責任，包括訂定及審批核證機關所採用的任何證書政策的權力及責任；

- 制訂有效程序以經常審核及更新核證作業準則；及
- 容許其登記人及倚據核證機關發出的認可證書的人仕查閱核證作業準則。

監察核證機關執行功能時遵守法例和監控規定：

5.10.2 認可核證機關需維持有效的機制以監察及確保遵守任何法律上及監控上的規定，包括條例及本業務守則的有關規定。

密碼匙管理

5.10.3 認可核證機關需對其本身的密碼匙的產生、儲存、備份、復原、分發、使用、銷毀及存檔維持有效的程序及方式，其中包括但不限於：

- 控制有關產生密碼匙加密模組的穩妥使用，包括採用符合適當保安標準的技術方案;
- 就產生密碼匙進行操作控制，其中包括但不限於：
  - 執行程序以確保用於產生密碼匙的設備保持完整性；
  - 執行程序以確保密碼匙是由授權人士在受監控的環境下產生；及
  - 若登記人的配對密碼匙由核證機關產生，核證機關必須執行程序以確保私人密碼匙以穩妥的方式及在沒有被更動的情況下交付登記人。私人密碼匙交付登記人後，除非登記人同意，否則核證機關不能存有登記人私人密碼匙的副本。
- 控制密碼匙的儲存、備份及復原，有關監控包括但不限於：
  - 定期測試核證機關的復原程序；
  - 執行程序確保核證機關的私人密碼匙得以穩妥地保管，例如只有在雙重控制下才可以存取。核證機關必須採取適當的措施確保能發現任何嘗試擅自取得核證機關的私人密碼匙的問題；及
  - 核證機關所有私人密碼匙的備份得以穩妥地在雙重控制下進行，而核證機關本身的私人密碼匙的備份應以穩妥的方式保存。

- 就分發密碼匙的程序作出保安控制(例如透過機制確保密碼匙的完整性及真確性，並監察密碼匙是否有任何改動)，包括但不限於：

  - 採取程序確保認可核證機關提供予署長在該核證機關披露記錄內存放的公開密碼匙的完整性及真確性；及

  - 採取程序確保核證機關本身的公開密碼匙的完整性及真確性。

- 對密碼匙的使用作出監控，包括啓動密碼匙的程序，例子包括但不限於：

  - 核證機關私人密碼匙的啓動應由多方控制，及可透過雙重認證才可啓動 (例如：實體權標加上密碼)；及

  - 核證機關的私人密碼匙只在規定的情況下，根據特定的目的及得到適當授權才可以啓動。

- 對配對密碼匙與任何有關的設施的安全銷毀作出控制，包括採取程序以確保能徹底銷毀私人密碼匙（令私人密碼匙在銷毀後再不能復原或重組）及撤銷原本配合已銷毀私人密碼匙的公開密碼匙。

- 採取監控措施，確保所保存的密碼匙符合其核證作業準則內的保安及運作規定。

產生密碼匙工具的管理：

5.10.4 認可核證機關必須就產生密碼匙工具的採購、接收、安裝、驗受測試、委托、使用、維修、保養及棄用，採取有效的政策、程序及控制。監控例子包括但不限於：

- 採取程序以確保加密工具的完整性，以免導致資料洩漏；

- 採取程序以確保產生密碼匙的工具由授權人士在適當的控制下操作，以防止工具遭擅自改動，並制訂控制機制以確保加密模組不會在不知情的情況下遭人擅自改動

- 採取程序確保使用加密模組產生的密碼匙的強度對核證機關及登記人來說能適合其使用密碼匙的目的。

由核證機關提供的密碼匙管理服務(如適用):

5.10.5 假如認可核證機關爲登記人提供密碼匙管理服務，如密碼匙的產生、儲存、備份、復原、銷毀、保存等，核證機關需爲這些服務制訂有效的政策、程序及控制措施。這些政策、程序及控制措施必須與本守則在第 5.10.3 及 5.10.4 段列出的原則一致。

權標的生命周期管理(如適用)：

5.10.6 認可核證機關需對其所使用的任何權標(如智能咭)的生產、預備、啓用、使用、分派及終止使用制訂有效的政策、程序及控制措施。

證書管理

5.10.7 認可核證機關需對證書的管理制訂有效的政策、程序及控制措施，其中包括但不限於下列例子：

- 認可核證機關必須根據有關核證作業準則規定的程序，對向核證機關申請發出認可證書或將認可證書續期的人士進行身分核實。核證機關亦必須就該人士的名稱的獨特性進行核實；
- 必須訂立適當程序，在證書到期前提醒登記人需要爲證書續期；
- 認可核證機關在發出其認可證書時，需採取開放及共通的界面，而證書的格式需在有關的核證作業準則中註明；
- 必須設立適當的政策及程序，以確保認可核證機關儲存庫的效能符合核證機關在其核證作業準則就儲存庫所訂立的服務水平；及
- 認可核證機關必須在其核證作業準則內訂明處理登記人投訴的程序。

證書撤銷清單的管理

5.10.8 認可核證機關需就證書撤銷清單的管理制訂有效的政策、程序及控制措施，其例子包括但不限於：

- 認可核證機關必須根據其核證作業準則的規定更新證書撤銷清單；及

- 制訂程序，以確保只有獲授權人士才能進入儲存庫和接觸證書撤銷清單以進行備存工作。

使用穩當系統產生密碼匙及保存紀錄

5.10.9 認可核證機關在產生本身及登記人的配對密碼匙時必須採用穩當系統。

5.10.10 認可核證機關必須分開保存其私人密碼匙及啓動數據(如個人辨認密碼、密碼等)，以確保其私人密碼匙及啓動數據得以穩妥保存，和在提取及進行檢查時能保持完整性及可供查察。

5.10.11 認可核證機關必須製備及儲存下列紀錄：

- 有關認可證書的發出、續期、暫時吊銷及撤銷的工作(包括任何人士向認可核證機關申請認可證書的身分證明文件)；
- 證書撤銷清單；
- 有關產生認可核證機關本身的配對密碼匙的文件；
- 有關產生登記人的配對密碼匙的文件；及
- 認可核證機關的電腦設施的行政管理紀錄。

這些紀錄必須以穩妥的方式儲存，並在提取及進行檢查時能保持其完整性及可供查閱。

5.10.12 認可核證機關需爲其發出的所有認可證書存檔，並設立查閱這些證書的機制。認可核證機關必須保存本部分所要求的所有紀錄，以確保若要將有關紀錄提供予署長或評估認可核證機關運作的人士時，該等資料是準確、完整、易讀及可供查閱。

數碼簽署

5.10.13 產生數碼簽署所採用的技術必須確保：

a. 數碼簽署必須在其相關的人士的指示下才能產生；及

b. 在與數碼簽署相關的人士沒有參與或不知情的情況下，任何人均不能複製該數碼簽署及從而建立有效的數碼簽署。

對穩當系統構成影響的事項

5.10.14 若發生任何事故對認可核證機關的穩當系統或其發出的認可證書造成重大及不利影響，該認可核證機關需：

- 就有關事故立刻通知署長；
- 採用合理的措施通知任何已知或可預見會受該事故影響的人士；及
- 如核證作業準則已訂明處理該類事故的程序，需按照這些程序行事。

5.10.15 認可核證機關須確保其所有員工具有適當的知識、技術資格和專業知識，以便有效執行他們的職責。

5.10.16 認可核證機關需確保其所有負責人員和賦與誠信職責的員工，如保安主管、核證機關行政主管、特別系統操作人員、登記人員、及其他能使用密碼匙資料、加密設施及工作事故紀錄的員工，均爲適當人選。

保安及風險管理

5.10.17 認可核證機關必須採用獲普遍接受的保安準則及標準制訂保安政策。

5.10.18 認可核證機關必須就其運作制訂全面的保安事故匯報和處理程序，及災難復原機制及程序。

5.10.19 認可核證機關必須充分確定及制訂程序，以處理其運作時所產生的風險，亦需實施風險管理計劃，以管理包括但不限於以下的事故：

- 密碼匙資料外洩；
- 核證機關的系統或網絡被入侵；
- 核證機關的基建設施無法使用；及
- 未經許可而製造證書及暫時吊銷和撤銷證書的資料。

6 證書及認可證書

6.1 認可核證機關可發出署長根據條例第 21 條所認可的證書或未經署長認可的證書。

6.2 認可證書內應載有所需資料，以方便登記人及依據證書的人士在進行電子交易時找到有關的核證作業準則。

發出證書

6.3 認可核證機關必須在以下情況才可向個人發出認可證書：

(a) 收到個人申請認可證書的要求；及

(b) 遵照核證作業準則內所規定的一切做法及程序，包括就關於該類型、類別或種類認可證書而核實申請人身分的程序。

6.4 認可核證機關必須讓登記人有合理機會在接受認可證書前先核實其內容。

6.5 認可核證機關必須在其設置或由外發機構設置的聯機及可供公眾查閱的儲存庫內公布其發出而又獲登記人接受的認可證書。

6.6 認可核證機關必須得到登記人的同意，然後把登記人的任何個人資料載入其發給登記人的證書及將證書在聯機和可供公眾查閱的儲存庫內公布。

6.7 認可核證機關一旦發出認可證書，而登記人又予以接受，認可核證機關必須在一段合理時間內，將其所知並影響認可證書有效性或可靠性的任何事實告知登記人。

6.8 認可證書必須註明有效期在何日屆滿。

6.9 認可核證機關發出認可證書，即屬向合理地倚據認可證書或認可證書內列出的公開密碼匙所能核實的數碼簽署的人士，表述該認可核證機關已按照該證書內以提述方式收納的適用的核證作業準則，或該核證機關已按照爲該人所知悉的核證作業準則，發出該認可證書。

6.10 凡與發出認可證書有關的事項，包括日期和時間，均必須以穩妥的方式記錄及保存，並確保在存取及查閱時，這些資料能保持完整性及可供查閱。

暫時吊銷及撤銷證書

6.11 認可核證機關必須能夠將認可證書撤銷，亦可以將認可證書暫時吊銷。

6.12 認可證書必須載有或以提述方式納入足夠資料，以便在該認可證書被暫時吊銷(如適用)或撤銷時，可以認定或確定會載列該認可證書暫時吊銷(如適用)或撤銷的通知的儲存庫。

6.13 除非認可核證機關及登記人協議採取其他做法，否則發出認可證書予登記人的認可核證機關必須在接獲以下人士的要求後，在一段合理時間內暫時吊銷(如可以將認可證書暫時吊銷)或撤銷有關的認可證書：

(a) 認可證書內指名或指出的登記人；或

(b) 獲授權代表該登記人行事的人士。

6.14 認可核證機關必須於暫時吊銷(如可以將認可證書暫時吊銷)或撤銷認可證書後的一段合理時間內，在其設置的儲存庫或由其他外發機構設置的儲存庫公布經簽署的暫時吊銷或撤銷(如證書撤銷清單)認可證書的通知。

6.15 認可核證機關撤銷或暫時吊銷證書(如可以將認可證書暫時吊銷)的時間，及在登記人或獲授權代表該登記人行事的人士提出撤銷或暫時吊銷證書要求時起，至證書確實被撤銷或暫時吊銷止的時間內，以該證書進行交易的責任分配問題，屬核證機關和登記人之間的服務協議安排，但這些安排需在有關的核證作業準則中列明。

6.16 若認可核證機關有合理理由相信所發出的認可證書不可靠，則無論登記人同意與否，認可核證機關可暫時吊銷(如可以將認可證書暫時吊銷)有關證書；但認可核證機關必須在一段合理時間內完成調查有關證書可靠性的工作，及決定是否恢復該證書的有效性或撤銷該證書。

6.17 若認可核證機關在考慮所有其擁有的證據後，認爲應即時撤銷所發出的認可證書，則無論登記人同意與否，有關證書應予以撤銷。

6.18 若登記人或獲授權代表該登記人行事的人士要求暫時吊銷認可證書(如可以將認可證書暫時吊銷)，則該認可核證機關必須在有關認可證書被暫時吊銷後，向該登記人或獲授權人士查詢是否應撤銷有關證書或恢復有關證書的有效性。有關的核證作業

準則必須列明進行該等查詢的預算期限，及如果認可核證機關未能聯絡該登記人或獲授權人士時所應採取的行動。

6.19 核證機關如暫時吊銷(如可以將認可證書暫時吊銷)或撤銷所發出的認可證書，必須在一段合理時間內，將認可證書已被暫時吊銷或撤銷之事，告知該認可證書的登記人或獲授權代表登記人行事的人士。

6.20 認可核證機關須提供熱線電話或其他設施，以供登記人舉報有關可能影響其證書或私人密碼匙的事項，例如：遺失密碼匙或密碼匙資料外洩。

6.21 凡與暫時吊銷或撤銷認可證書有關的事項，包括日期和時間，均必須以穩妥的方式記錄及保存，並確保在存取及查閱時，這些資料能保持完整性及可供查閱。

認可證書的續期

6.22 認可證書可在有效期屆滿時，根據登記人的要求及由認可核證機關決定續期。

6.23 凡與認可證書續期有關的事項，包括日期和時間，均必須以穩妥的方式記錄及保存，並確保在存取及查閱時，這些資料能保持完整性及可供查閱。

7 登記人身分的核證

7.1 認可核證機關必須在與某類型、類別或種類的認可證書有關的核證作業準則內，列明向該認可核證機關申請這些認可證書人士的身分核實程序。

7.2 認可核證機關必須保存能證明其登記人身分的書面證據。

8 倚據限額

8.1 認可核證機關向登記人發出某類型、類別或種類的認可證書時，可在有關某類型、類別或種類證書的核證作業準則內訂明倚據限額。核證機關必須在核證作業準則訂明使用該等證書時倚據限額的含意。

8.2 認可核證機關必須作出適當安排，確保其能夠對不超逾其發出認可證書所訂明的倚據限額的索償要求承擔責任。

9 儲存庫

9.1 認可核證機關必須最少提供一個由其設置或由外發機構設置的聯機及可供公眾查閱儲存庫，以公布認可證書及其他資料。認可核證機關必須確保其儲存庫是由一套穩當系統提供，並在其核證作業準則內明確列出有關其儲存庫運作的服務水平。

9.2 認可核證機關在設置及管理儲存庫時，不得進行任何對倚據認可證書及儲存庫所載的其他資料的人士造成不合理風險的活動。

9.3 認可核證機關的儲存庫必須載有以下資料：

- 由核證機關發出的認可證書；
- 暫時吊銷(如適用)或撤銷認可證書(包括證書撤銷清單(如適用))的通知；
- 該認可核證機關的核證機關披露紀錄；
- 署長指定的其他資料。

9.4 認可核證機關的儲存庫不能載有其所知爲不確或在合理情況下屬不可靠的資料。

9.5 認可核證機關必須在其儲存庫內把過去最少七年內被暫時吊銷或撤銷，或有效期屆滿的認可證書存檔。

10 披露資料

10.1 認可核證機關必須在其儲存庫內公布：

(a) 載有其公開密碼匙的核證機關證書，而該公開密碼匙與該核證機關用以爲它發出的證書進行數碼簽署的私人密碼匙對應；

(b) 有關其核證機關證書或署長所給予的認可資格被暫時吊銷、撤銷或不獲續期的通知；及

(c) 對認可核證機關所發出的認可證書的可靠性或認可核證機關提供核證服務的能力，造成重大及不利影響的任何其他事實。

10.2 若認可核證機關在聘用負責人員或任何與負責人員有相同職能的人員方面有任何轉變，必須在該人員受聘日期起計三個工作天內通知署長。

10.3 認可核證機關必須每六個月，向署長呈交載有以下資料的進度報告：

(a) 每類型、類別或種類證書的登記人的數目；

(b) 所發出、暫時吊銷、撤銷、有效期屆滿及獲得續期的每類型、類別或種類證書的數目；

(c) 工作表現與既定服務水平的比較；

(d) 所發出新類型、類別或種類的證書；

(e) 組織結構或系統的改變；及

(f) 自上次呈交進度報告或申請認可以來，以上各項資料的改變。

10.4 以上資料如有任何改變而又值得署長注意，認可核證機關亦必須立即向署長披露。在有需要的情況下，署長亦可隨時給予一段合理時間的通知，要求認可核證機關呈交這方面的報告及其他與條例有關的資料。

10.5 認可核證機關必須向署長即時報告任何可以或會就其核證機關運作產生潛在利益衝突的事項。

10.6 認可核證機關必須向署長即時報告可能對其運作構成影響的任何特別事故。

11 終止服務

11.1 認可核證機關於申請認可或續發認可時，必須向署長提交一份終止服務計劃。

11.2 終止服務計劃必須指明核證機關終止服務時的安排，尤其是存檔爲期不少於七年的紀錄的安排。紀錄包括其所發出的證書及

核證機關證書，以及確保以妥善方式儲存檔案，並在存取及查閱時，這些檔案能保持完整性及可供查閱。

11.3 終止服務計劃應包括核證機關服務的自願及非自願終止，及由署長對核證機關所給予的認可到期或遭撤銷。終止服務計劃亦必須包括有關措施，以確保在核證機關終止服務時，登記人的利益能得到妥善保障。

11.4 終止服務計劃屬核證機關核證作業準則的一部分。

11.5 如認可核證機關擬終止運作，必須

(a) 在終止其核證服務前不少於 90 日內通知署長；

(b) 在終止其核證服務前不少於 60 日內通知其全部登記人；

(c) 在終止其核證服務前不少於 60 日內，最少連續三日在一份本地英文報章及一份本地中文報章刊登有關擬終止服務的啓事；

(d) 如署長認爲有需要，在核證機關終止其核證服務時，無需考慮登記人有否提出撤銷證書的要求，撤銷所有尚未撤銷或有效期仍未屆滿的證書；及

(e) 提供適當的安排，令核證機關資料庫內的資料，包括所發出的證書及核證機關的公開密碼匙，得以順利轉移。

12 對遵守條例及本業務守則的評估

12.1 認可核證機關必須最少每十二個月向署長提交一份報告，而該報告須載有對該核證機關在所擬備的報告所涵蓋的期間是否已遵守條例中適用於認可核證機關的條文的評估，及在該期間是否已遵守業務守則的評估。

12.2 所有評估必須由署長爲此目的核准的合資格獨立人士執行。執業會計師，即指根據《專業會計師條例》(第 50 章)持有執業證書的專業會計師(並在需要時由資訊科技的專業人士支援)，屬可獲署長接受及核准爲制備報告的人仕。署長在適當時亦可考慮其他人士是否合資格制備報告。

12.3 核證機關必須在評估完成後四個星期內將一份評估報告呈交署長。如認可核證機關向署長申請將認可續期，該核證機關必須呈交在提出續期申請日前三個月內完成的評估報告。

12.4 署長可根據認可核證機關未能通過評估爲理由，暫時吊銷或撤銷其獲給予的認可資格，或拒絕有關核證機關提出將認可續期的申請。

12.5 有關評估的進一步資料請參閱附件三。

13 標準及技術的採用

13.1 認可核證機關必須不斷檢討及適當更新所採用的標準和技術，以維持登記人對其的信心及保障登記人的權益。

14 互通性

14.1 爲減少對認可證書所支援的數碼簽署的障礙以促使其獲得廣泛接受，認可核證機關必須盡可能採用開放及共通界面，以協助其他人核實其發出的認可證書所證明的數碼簽署。

14.2 認可核證機關必須在有關的核證作業準則內，指明其所支援的開放和共通界面，及與其他核證機關所建立的互通安排。

15 保障客戶

15.1 認可核證機關就其服務所作的宣傳必須正確及真實。在廣告內作出比較時亦應是公平和不會產生誤導作用。所有聲稱必須是可以證實的。

核證機關及證書的認可

引言

1 凡向署長申請認可的核證機關必須能夠遵守條例內適用於認可核證機關的條文及本業務守則。認可核證機關並且可以向署長申請給予證書認可。

2 本附件概述申請成爲認可核證機關及給予證書認可的條件和程序。

核證機關的認可

3 根據條例第 20(3)條，在決定申請人是否適合認可時，署長除考慮其認爲有關的任何其他事宜以外，還須考慮以下事宜--

(a) 申請人的財政狀況是否讓其在遵從條例適用於認可核證機關的條文及本業務守則的情況下運作；

(b) 申請人已作出的或擬作出的應付因其與本條例的目的有關的活動而可引致的法律責任的安排；

(c) 申請人使用的或擬使用的用作向登記人發出證書的系統、程序、保安上的安排及標準；

(d) 一份載有對申請人是否有能力遵守條例適用於認可核證機關的條文及本業務守則的評估的報告；

(e) 申請人及負責人員是否適當人選；及

(f) 申請人爲其證書設定的或擬爲其證書設定的倚據限額。

財政狀況

4 條例第 20(3)條第(a),(b)及(f)段提及有關申請人在財政方面的運作。

5 申請人需提供以下證明--

(a) 評估該核證機關運作上將會或已出現的商業和財政風險；亦已作出適當的安排去保障該核證機關本身的運作或在運作上可能產生的法律責任。如核證機關在其發出的證書內指明倚據限額，核證機關應該備有充分保險去應付可能產生的法律責任；及

(b) 核證機關意圖和將保持持續經營。此意圖可以多類的方式表明，包括但不受限制於--

- 維持足夠財務安排以支持其運作；
- 已裝置或準備裝置核證機關運作時所需要的系統及設備及作出所需的財務安排；及
- 無論是在質素(以技能而言)及數量(以人數而言)方面都已僱用足夠之員工，以支持核證機關之運作及作出所需的財務安排。

系統、程序、保安上的安排和標準

6 政府只會認可一些達到政府能接受的穩妥水平的核證機關。因此申請人必須能夠證明其系統、程序、保安安排和標準能組織成一個穩當系統，透過該系統核證機關向登記人發出證書和從事其它有關活動。

7 在本業務守則第五項詳述關於穩當系統的指引。

評估認可核證機關的報告

8 認可核證機關必須最少每十二個月向署長呈交報告一次，而該報告須載有對該核證機關在所擬備的報告所涵蓋的期間內是否已遵守條例中就適用於認可核證機關的條文的評估，及在該期間內是否已遵守本業務守則的評估。

9 所有評估必須經由署長爲此目的而批準的合資格獨立人士進行。執業會計師是合適的人士獲得署長批准從事評估報告的擬備工作。執業會計師是根據《事業會計師條例》〔第 50 章〕持有執業證書的專業會計師，及在需要時由資訊科技專業人員支援。署長亦可考慮其他人士是否具備合適的資格去擬備評估報告。

適當人選

10 根據條例第 20(3)條(e)段，申請人及其負責人員必須爲適當人選。條例第 20(4)條列出適當人選的標準。申請人必需在申請認可時聲明本身及其負責人員是適當人選。

核證機關的認可有效期

11 一般核證機關的認可有效期爲 2 年。核證機關可在其認可有效期屆滿日前 30 天至 60 天的期間內向署長申請將認可續期。

證書的認可

12 認可核證機關可向署長申請就其發出的所有或部分證書給予認可。假如核證機關不是認可核證機關，該核證機關可以將其核證機關認可申請和證書認可申請一同遞交。署長將先考慮核證機關的認可申請，然後才考慮其證書的認可申請。

13 一般而言，如果核證機關的認可保持不變及其發出的核證作業準則，包括用以規定認可證書的有關證書政策(如可容許)不存在重大的改變，證書的認可將不會改變。

14 影響證書的認可包括以下重大的改變 --

(a) 身分核證程序改變並削弱證書的可靠性；

(b) 證書的倚據限額改變；或

(c) 對密碼匙的產生、儲存、及其使用的要求的改變。

證書認可準則

15 認可核證機關在申請某類型、類別或種類的證書的認可時需要證明-

(a) 證書是按照核證機關的核證作業準則發出；

(b) 證書是按照業務守則發出；及

(c) 核證機關已作出的或擬作出充分的安排以應付因其發出該類型、類別或種類的證書而可引致的法律責任。

有關核證作業準則內容的指引

引言

1 條例及業務守則(下文簡稱「守則」)要求認可核證機關除遵守其他規定外，必須：

- 發出及備存最新的核證作業準則[1]；及
- 通知署長有關核證作業準則上的轉變。

2 本附件就核證作業準則的內容提供指引，認可核證機關須以此作爲最基本的參考。

3 我們必須特別注意，核證作業準則是專爲特定核證機關的組織架構、操作程序、設施、電腦作業環境及核證機關發出證書的有關證書政策而設。因此，核證作業準則的詳細程度及其每段的特徵，將因應不同的核證機關而有所不同。

4 本指引的內容主要以網絡工程工作小組(The Internet Engineering Task Force)第 2527 號 RFC 文件「證書政策及核證作業架構」(Certificate Policy and Certification Practices Framework)(一般稱爲 IETF PKIX 第四部分)作爲基礎。然而，我們無意以此作爲核證作業準則指引的唯一有關來源。

[1]核證作業準則的概念首先在美國律師公會數碼簽署指引(American Bar Association Digital Signature Guidelines)中獲得明確闡述。美國律師公會的指引把核證作業準則界定爲「核證機關用以發出證書的作業準則」。選用這個詞語的部分原因，是防止其與「政策」一詞造成含糊或混亂。核證作業準則不應與證書政策混淆，因爲兩者就作者、目的、具體程度及方法等方面均各有不同。

附錄：核證作業準則的建議涵蓋範圍

1 特徵概述

在本部分，核證機關必須考慮就其所發出的證書的類型、類別或種類的主要特徵作出概述。本部分的目的是讓核證機關用戶能迅速了解根據核證作業準則發出的證書的有關因素。

該等特徵必須包括每類型、類別或種類證書的認可情況、其有關的倚據限額，及其他重要特徵如可影響登記人或倚據證書人士對證書的信心及信任程度的所需的鑑別方式。本部分應包括網址或其他來源的引述，而有關網址及來源是指出核證機關保存有關其認可狀況資料的地方，及其由署長備存的核證機關披露紀錄的地方。

2 引言

2.1 概論

核證作業準則目的及範圍的最高層次概論，包括其認可的範圍，例如有否附上任何條件，及概述認可對於登記人及倚據人士的意義。本部分亦可指出核證機關服務的範圍、條款及條件。

2.2 鑑別

核證機關如不就其發出的證書尋求認可，便不需要認定任何支持的證書政策。但如果核證機關支持特定的證書政策或就其發出的任何證書尋求認可，則必須在此指出該等政策並提供適當的證書政策物件辨識項目。另外，核證機關須確保所識別的政策全文刊登在登記人及預期的登記人可聯機接達的地方。

2.3 群體及適用性

本部分必須指出所有形成或參與核證機關運作及維持核證機關的已知群體及功能。其中包括核證機關功能、註冊功能、儲存庫，及其目標終端用戶(如登記人)。假若核證機關其中一個或一個以上的主要功能屬外發形式提供，如使用第三者註冊功能，必須在本部分清楚列明。

本部分亦必須列明對核證機關發出每類型、類別或種類證書所適用的限制，其中包括：

- 所發出證書的適用情況，例如：電子郵件、零售交易、合同等；
- 已發出證書在使用上的限制；及
- 已發出證書在使用上的禁制。

2.4 聯絡資料

核證作業準則必須最少列明一個可與該核證機關聯絡的通訊地址，以便回答登記人、監管機構及其他查詢。一般來說，核證機關最少列出一個電話號碼、郵遞地址及電子郵件地址供登記人和倚據證書人士聯絡該核證機關。另外，核證作業準則必須向登記人提供服務熱線的資料，以便登記人報告資料如報告密碼匙遺失等。

3 一般條文

3.1 責任

3.1.1 核證機關的責任

本部分需清楚列出核證機關爲其提供的服務承擔的責任包括條例訂立的特定責任，其中包括其認可條件及業務守則。該等責任的例子包括：

- 通知(包括作出該等通知的時間)登記人證書的發出，而該登記人需是所發出證書的對象；及
- 通知(包括作出該等通知的時間)登記人其證書已遭撤銷或暫時吊銷。

如認可核證機關以外發形式執行其任何功能，該等功能的有關責任須另作描述。

3.1.2 登記人責任

本部分應描述根據核證機關所支持的證書政策所指定給予其登記人的職責及責任，例如：

- 確保在申請證書時陳述準確；
- 保障登記人的私人密碼匙；

- 限制私人密碼匙及證書的使用；及
- 就私人密碼匙資料外洩作出通知。

3.1.3倚據人士責任

本部分應根據核證作業準則，包括核證機關所支持的任何證書政策，清楚指出對倚據人士作出的所有申述：

- 清楚明白使用該證書的目的；
- 核證數碼簽署的責任；
- 檢查證書遭撤銷及暫時吊銷的責任；及
- 確認接受適用的責任限制及保證。

3.1.4儲存庫責任

本部分需清楚列出核證機關就提供儲存庫服務所承擔的責任，包括條例訂立的特定責任，其中包括其認可條件及業務守則。該等責任的例子可包括按時公布證書及撤銷證書(包括暫時吊銷證書)的資料。

3.2 法律責任

核證機關需清楚列明任何有關攤分責任適用的條款，包括處理由證書支持的交易，而該等交易在登記人要求撤銷或暫時吊銷證書與核證機關實際撤銷或暫時吊銷期間發生。核證機關亦必須清楚指出所列明的倚據限額的含意。在任何情況下，本部分的任何部分均不應豁免，或保障核證機關豁免任何法律上不能豁免的責任。

3.2.1保證及保證的限制

核證機關必須就其所發出的每類型、類別或其他種類的證書清楚列明其有意採用的任何保證及/或限制。

3.2.2賠償責任及拒絕賠償

核證機關必須就其所發出的每類型、類別或種類的證書，清楚列明其負責的賠償(例如：間接的、特別的、相應的、突發的、懲罰性的、算定損害賠償、疏忽及欺詐)及任何拒絕賠償事項及責任限制的範圍。

3.2.3損失限制

核證機關必須就其所發出的每類型、類別或種類的證書，清楚列明有關每張證書或每項交易的損失限制。

3.2.4其他豁免

核證機關必須就其所發出的每類型、類別或種類的證書清楚列明其他適用的豁免。

3.3 財務責任

本部分應指出有關核證機關及其他任何在核證作業準則認定的人士的財務責任，其中可以指出的範圍包括：

- 受信關係會否在核證作業準則所認定的人士之間出現，或會因發出證書的活動而預期產生；
- 有關行政程序的財政責任；
- 核證機關爲其證書倚據限額就潛在或實際責任及索償對登記人及倚據人士所作出的財務保證；及
- 其他任何方面的財務範圍，如表現擔保金，保險單或其他由認可程序引致的責任(如認可條件)。

3.4 闡述及執行

3.4.1主管條例

核證作業準則必須指明核證機關及有關核證作業準則，登記人協議及倚據人士協議的司法管轄區。

3.4.2條文的劃分、保留、合併及通知

本部分必須指出，如發現核證作業準則其中一個或以上的部分有不合法、不能執行或無效的情況，其他部分仍維持有效。任何所找到的事項或問題必須立即予以處理。

3.4.3 解決爭議程序

本部分必須指出核證機關所制訂的，用以解決有關其運作及對於其登記人或倚據人士所作的陳述所引致的爭議及索償的程序。該等程序必須最少指出向核證機關提出爭議或索償的程序，及核證機關在接獲索償或爭議通知後所採取的步驟。

3.5 收費

本部分必須就核證機關發出的各類別、類型或種類的證書，明確指出對其登記人及倚據人士所收取的費用及收費。

3.6 公布及儲存庫

本部分應指出核證機關對其登記人及倚據人士傳達有關其核證作業準則資訊所採用的政策及機制，其中包括核證機關所支持的任何證書政策細節，及其發出證書的現行認可狀況。這須包括例如公布辦法、公布次數、資訊是否可供取閱、存取資訊的控制及儲存庫的細節。

核證作業準則的全文，或一份刪去運作細節以免對核證機關及其組成部分的完整性產生負面影響的刪短版本，應在核證機關的網頁及其他可以方便到達的地方清楚展示出來。

由於核證機關所依循的實際程序能合理地預期會出現進展，核證作業準則的更新內容必須適當地發布。所有變更必須在展示核證作業準則的同一地方展示出來。

3.7 關於遵守規定的評估

本部分必須指出有關核證機關遵守情況評估的機制及次數，包括根據條例及業務守則的強制性要求。具體範圍可包括：

- 核證機關及其任何以外發形式執行的功能的遵守情況評估次數；
- 獨立評估人的身分或資歷；
- 評估人與被評估機構的關係；
- 評估內容涵蓋範圍概要；及
- 有關傳達遵守規定的評估結果的政策(即報告文本的收件人)及跟進行動的政策。

3.8 保密政策

本部分必須指出核證機關備存資料保密的政策，需特別提及的事項包括：

- 核證機關需要保持機密的資料類型，包括任何以外發形式執行的功能；
- 不屬機密的資料類型；
- 就證書撤銷或暫時吊銷原因需要通知的人士；
- 發放資料的政策，如提供給執法人員，在法律程序下被要求披露等；
- 核證機關，包括任何以外發形式執行的功能，可以因應資料擁有人的要求/同意而披露資料的情況；及
- 其他可以披露機密資料的情況。

總括來說，核證機關必須遵守任何有關私人資料私穩的規例，核證作業準則的條文不能抵觸香港現行的有關私穩的規例及條例第 41 條。

3.9 知識產權

本部分提到關於證書、證書的資料結構、核證作業準則、作業/政策規定、名稱及密碼匙的知識產權。

4 鑑別及核實

本部分列出核證機關或其外發的註冊機構功能(如適用)所訂立的程序，以便在發出證書前核實登記人。本部分需描述核證機關所發出的每類別、類型或種類證書。

本部分亦必須包括證書調整或在撤銷後證書調整的核實程序，亦應指出核證機關有關命名的作業方式，例如命名權、名稱爭議及解決爭議的方法。

核證機關必須在核證作業準則內列明其接受的身分證明文件，例如:香港身分證、護照或公司章程等。

4.1 初步核證

本部分提到在發出新證書時有關身分鑑別、認證及命名的程序。本部分應指出在鑑別證書申請人身分時，核證機關必須採取特定程序，包括在發出證書予最終持有人前，要求個人或團體所需呈交的特定文件。

4.1.1 名稱種類

本部分應列出核證機關所採用的命名常規，如 X.500 Distinguished Names (獨特名稱)或其他方式的獨特名稱，如在網絡證書的命名。其他的命名方式，包括電子郵件地址或個人認證號碼，亦確保個人獲取證書時不會出現含糊的情況。

本部分亦必須列明所有命名方式的細節，包括可能會採用的前綴及常規，以預防名稱的抵觸。

4.1.2 名稱應具意義

本部分必須指出證書內的名稱是否應該具有意義。如證書內的名稱應該具有意義，則應列明核證機關爲此所訂立的程序，以確保所發給登記人的獨特名稱具有意義並能適當地確認登記人。

4.1.3 解釋不同命名形式的規則

本部分應包括根據核證作業準則發出的證書內名稱格式的闡釋指引。這範圍的深度取決於證書內的名稱格式。一般來說，如證書內名稱的闡釋有可能爲倚據人士誤解，核證機關應考慮向倚據人士提供指引以減少產生誤會的風險。

4.1.4 名稱的獨特性

如證書的名稱必須獨有的話，核證機關必須列出這項規定。在這種情況下，核證機關應披露其規定或任何適用的統一命名規則以確保特定名稱的獨有性。

4.1.5 解決命名索償爭議的程序

本部分必須適當地指明核證機關的解決命名爭議的程序。

4.1.6 證明擁有私人密碼匙的辦法

如果登記人自己產生其配對密碼匙，並獨有地控制其私人密碼匙，核證作業準則必須指出核證機關如何核實登記人的私人密碼匙與呈交核證的公開密碼匙對應。

4.1.7登記人身分的核實

本部分必須指出核證機關爲確保證書上的姓名與獲發證書的人士符合所作出的程序。本部分的主要目的是促使登記人能明白根據本核證作業準則取得數碼證書所需的要求，及促使倚據證書人士明白在本核證作業準則下所發出的證書的可靠性並對此作出結論。

4.2 例行調整及證書續期

本部分描述核證機關爲例行調整及證書續期所採取的程序，特別是如果該等鑑別登記人身分的程序與證書首次註冊及發出時不同。核證作業準則必須指出證書是否可不作調整而續期。本部分亦必須指明在證書有效期屆滿時，核證機關會否採取與首次發出證書時不同的程序。

4.3 撤銷後調整

本部分必須指出核證機關在撤銷證書後，會否採用與首次發出證書時不同的程序。如核證機關會採用不同的程序，該等程序必須在核證作業準則中詳細列明。

4.4 撤銷要求

本部分須列出核證機關在認證及處理撤銷要求時所採取的程序及機制，例如：

- 誰獲授權提出撤銷證書的要求及在何種情況下能提出此要求；
- 撤銷證書的影響；
- 撤銷證書後證書有效狀況的資料會在何時公布；
- 登記人就報告需要撤銷證書的事件的責任；及
- 在提出撤銷證書要求時對登記人所給予的保障，包括核證機構與登記人的責任攤分。

4.5 暫時吊銷要求

本部分應指出核證機關是否提供暫時吊銷證書的服務，如核證機關提供這項服務，則需詳細列出暫時吊銷證書的情況及影響。核證作業準則需具體指明暫時吊銷的實行方法，亦可適當地提及在第 4.3 段就撤銷所確定的相同因素。

5 操作要求

5.1 申請證書

核證機關應在本部分詳細列出登記人取得新證書的程序，包括：

- 登記人申請證書的方法及必須提交的文件，以證實登記人的身分；
- 提供予登記人的資料(其中包括但不限於登記人的責任，核證機關所作出的陳述、證書的條款及條件，核證機關及證書的認可狀況及其對登記人的影響，特別是不獲資訊科技署署長認可的證書)；及
- 證書要求的界面規定。

5.2 發出證書

在本部分，核證機關應詳細列明其在發出證書時所依循的程序。發出證書的程序應包括：

- 密碼匙的產生；
- 把密碼匙分派給合適人士(例如密碼匙由登記人所產生，該公開密碼匙應與申請證書的要求送交核證機關，而核證機關須核實登記人持有配對的私人密碼匙。如密碼匙由核證機關所產生，私人密碼匙應穩妥地送交登記人，而核證機關須列明有關的措施以確保其所保存的密碼匙得到適當的處理)；
- 在未取得登記人同意的情況下，核證機關不得持有登記人的私人密碼匙；
- 證書的產生；

- 送交證書給登記人；及
- 在儲存庫刊登證書。

5.3 接受證書

登記人接受證書的方式乃透過行動表現在履行登記人的職責及潛在的責任。在本部分，核證機關必須界定有關的技術或程序，以：

- 按照第 3.1.2 節所指出，向登記人解釋其責任；
- 通知登記人證書的產生及證書的內容；
- 要求登記人確認接受責任及證書；及
- 協助登記人從核證機關獲得數碼證書。

5.4 暫時吊銷及撤銷證書

在本部分，核證機關須解釋進行暫時吊銷證書（如證書可遭暫時吊銷）與撤銷證書的程序。本部分應包括登記人或其他獲授權人士指示核證機關暫時吊銷或撤銷證書時會採取的程序。

5.4.1 暫時吊銷證書(如證書可遭暫時吊銷)

核證機關須在本部分列出暫時吊銷證書的詳細程序，包括：

- 暫時吊銷證書的情況(包括但不限於誰可以指令/撤回暫時吊銷證書)；
- 要求/指令暫時吊銷證書的方法；
- 通告暫時吊銷證書的方法(如透過張貼通告、電子郵件或在證書撤銷清單內列出遭暫時吊銷的證書)；
- 撤回暫時吊銷或由暫時吊銷過渡到撤銷的情況，例如：時限；
- 認可核證機關暫時吊銷認可證書的時間，以及在登記人或獲授權代表登記人行動的人士要求暫時吊銷證書及證書實際遭暫時吊銷之間的時間利用證書進行交易的責任攤分；

- 有關的核證作業準則必須界定預計時限，以便核證機關在此時限內向登記人或獲授權人士查證遭暫時吊銷的認可證書在暫時吊銷後是否會遭撤銷或恢復其有效性；及

- 如認可核證機關不能接觸登記人或獲授權人士以確定該遭暫時撤銷證書的最終安排時，核證機關所採取的行動。

5.4.2 撤銷證書

核證機關應在本部分列出撤銷證書的詳細程序，包括：

- 撤銷證書的情況(包括但不限於誰可指令/撤回撤銷證書)；

- 要求/指令撤銷證書的方法；

- 作出撤銷通知的方法(如透過張貼通告、電子郵件或在證書撤銷清單內列出遭撤銷的證書，或更新載有撤銷證書/證書是否有效的資料的伺服器)；及

- 認可核證機關撤銷認可證書的時間，以及在登記人或獲授權代表登記人行動的人士要求撤銷證書及證書實際遭撤銷之間的時間利用證書進行交易的責任攤分。

獲授權人士可使用能辨別將被撤銷的證書、解釋撤銷證書的理由及可以核實撤銷證書要求(如數碼或人手簽署)的界面，提出撤銷登記人的證書。核實撤銷證書的要求十分重要，因爲這措施可以防止未獲授權人士惡意撤銷證書。傳送資料的方法如電子郵件及網絡界面，應隨時可供登記人使用。

一般來說，證書在下列情況下須予以撤銷：

- 使用者證書上的鑑別資料或特徵在證書到期前有所改變；

- 知悉證書的對象已違反發出證書的核證機關適用的核證作業準則所載規定；

- 登記人懷疑或確定私人密碼匙的資料外洩；或

- 使用者不再希望擁有或需要簽署電子訊息的能力。

5.4.3證書撤銷清單

證書撤銷清單載列未過期但不再有效的證書，及其被撤銷的理由。在核證作業準則內應列明分發證書撤銷清單的機制，及倚據人士如何取得該清單或其他機制以確認個別證書的認可狀況。

核證機關須在這部分指明更新證書撤銷清單的頻密程度，並可決定使用或支援額外機制以核實證書是否有效。核證作業準則須指明可供使用的機制，其使用的條款和條件及如何取得資料。

5.4.4查核證書撤銷清單的規定

核證機關必須通知登記人及在一般可以到達的地點顯眼地張貼通告，指出如載有公開密碼匙的證書不再有效，倚據其數碼簽署是存在風險的。倚據人士如不核實證書是否有效，則需要承擔一切風險。

在此部分，核證機關必須指明倚據人士應透過查核證書撤銷清單或採用由核證機關支持作核實證書的其他同等機制，檢查證書的有效性。

核證作業準則亦須清楚地及明顯地指出，在倚據人士暫時不能取得撤銷資料的情況下其政策的內容。核證機關可以特別指出在這種情況下各方面的承擔情況。

5.5 保安審核程序

本部分旨在描述核證機關應採用的記錄事件及監察的系統，以達至維持保安環境的目的。應包括的要素如下：

5.5.1紀錄的事件類型

本部分描述核證機關所紀錄的事件類別。基本上，核證機關應考慮紀錄下列事件：

- 網絡上一切有可疑的活動；
- 多次未能使用系統的情況；
- 關於核證機關的運作設備及軟件的安裝、修改及配置的事項；
- 特許使用核證機關的各部分；及
- 一般證書管理的操作，例如：

- 要求撤銷及暫時吊銷證書；
- 實際發出、撤銷及暫時吊銷證書；
- 證書續期；
- 更新儲存庫；
- 證書撤銷清單的產生及刊登；
- 核證機關密碼匙的密碼轉換；
- 備份；及
- 緊急復原密碼匙。

所紀錄的事件應盡可能列出有關報告的機構或個人，及任何曾作出的相應行動及由誰作出該等行動。所有記下的紀錄必須蓋上日期及時間的蓋章。

核證機關首先根據現行獲採納的運作模式，對個別與保安有關的事件和趨勢的嚴重性及重要性訂立界線，是良好的作業方法。所有超出界線的事件和主要趨勢必須加以記錄。

核證機關必須實施特許權的劃分及其他機制或程序，以確保所有紀錄的完整。用以實施特許權劃分的機制及程序，應在核證作業準則內列明。

5.5.2處理事件紀錄的頻密程度

本部分列明進行事件紀錄的頻密程度，例如綜合審核及檢討。

5.5.3事件紀錄的保存期限

本部分列明事件紀錄的保存期限，應符合業務守則的要求。

5.5.4保障事件紀錄

本部分列明應爲保障事件紀錄免受意外損毀或蓄意的修改而採取的機制。

5.5.5事件紀錄備份程序

本部分列明應替事件紀錄進行備份的程序及其保留期限。良好的備份模式，是確保儲存地點能提供足夠的保障以避免盜竊、損毀或媒體衰變。另外，必須確保在存檔期間存取數據的方法是現行的有效方法。

5.6 紀錄存檔

本部分旨在描述關於核證機關保留紀錄的政策。根據一般規定，核證機關須確保其所存檔的紀錄詳盡程度，必須足以在特定時限內確認證書的有效性及核證機關的妥善運作。核證機關可考慮存檔資料包括：

- 關於核證機關的設備的資料，如：
  - 核證機關系統設備配置檔案；
  - 核證機關的評估或審核（如需要）的結果；
  - 核證作業準則；及
  - 制約核證機關的任何合約性質的協議。
- 關於核證機關操作的資料：
  - 任何上述項目的修改或更新；
  - 所有已發出或公布的證書及證書撤銷清單(或其他撤銷資料)；
  - 定期的事件紀錄(根據第 5.5 段)；及
  - 其他核實存檔內容的所需資料。

5.6.1存檔的保留期限

本部分列出存檔紀錄的保留期限，應符合業務守則的規定。

5.6.2保障存檔

本部分列出保障存檔紀錄的程序，其中包括：

- 該等存檔的保管人；

- 取得該等紀錄的機制，例如爲審核或解決紛爭的用途；及

- 保障存檔免受意外損毀或蓄意修改、盜竊或媒體衰變。

5.6.3存檔備份程序

本部分列出爲存檔紀錄進行備份的程序及其保留期限。良好的操作模式是要確保儲存地點能提供足夠的保障以避免盜竊、損毀或媒體衰變。另外，必須確保在存檔期間儲存及存取數據的方法是現行的有效方法。

5.7 密碼匙變更

本部分描述核證機關變更密碼匙的詳情及通知登記人有關程序的機制。

5.8 密碼外洩及災難復原

本部分描述在密碼外洩或災難時，核證機關在發出通知及復原程序的要求。核證機關必須特別提及下列事項：

- 核證機關在其電腦資源、軟件，及/或資料遭破壞或洩漏的情況下，或懷疑遭破壞或洩漏的情況下所採取的復原程序。該等程序描述如何重新建立穩妥的環境、那些證書應遭撤銷、核證機關本身的密碼匙應否撤銷、如何爲登記人提供新的核證機關公開密碼匙及如何再核證登記人；

- 核證機關遇上密碼匙資料外洩或懷疑外洩時所採取的復原程序，包括通知登記人和倚據人士，及重建核證機關穩當信譽的程序；及

- 核證機關在自然或其他災害後，及重新建立穩妥環境期間爲其設備在原地點或後備地點進行穩妥保存的程序。例如在受損毀的地點保護敏感材料免遭盜竊。

如發生任何上述事項應立即通知署長。

5.9 核證機關終止服務

本部分指出核證機關終止服務及通知其登記人及倚據人士終止服務的程序安排，包括核證機關存檔紀錄的保管人身分。該等安排應符合業務守則第 11 條所列出的要求。

6. 實體、程序及人事保安管制

本部分列明核證機關確立的非技術性運作管制措施，以確保其業務以穩當的方式進行。

該等管制的例子包括就核證機關主要功能的實體、程序及人事的管制，如密碼匙的產生、認證、發出證書、撤銷證書、審核、存檔等。關於儲存庫及任何以外發形式執行的功能(如註冊功能)，核證機關亦可制訂類似管制。

6.1 實體保安管制

本部分列明管制裝載核證機關系統的設施的詳情，其中包括：

- 場地位置及建設；
- 認定保安範圍及實質進入範圍的考慮；
- 環境災患，例如電力供應、冷氣、濕度、水災、火災等；及
- 媒體儲存及銷毀。

6.2 程序控制

獲信任角色指在該職位的人士無論是因意外或蓄意而引致不恰當地執行其職責，便可能會出現保安問題。獲信任角色包括由核證機關管理層監察的負責人員及操作員工，獲得選擇擔當此職位的人士應當具備所需才能及足以勝任。該等職務的功能是整個核證機關信任的基礎。

本部分列明核證機關認定獲信任角色的程序，例如產生核證機關密碼匙，界定該等職位的責任。一般來說，該等程序的規定將列出需要執行的任務、執行每個任務所需的人員數目及職位，及所實施的管制如雙向管制、認定及核實有關人士等。

典型的獲信任角色可以包括：

- 核證機關的行政人員—該等人士監察所有證書的發出、核證機關的運作及收集及備存紀錄。基本來說，核證機關的行政人員必須確保核證機關功能依循核證機關核證作業準則內的規定；
- 密碼匙復原代理人-負責有關備存密碼匙復原代理人材料或系統具體功能的個人; 及

- 其他獲信任角色—核證機關可在其行政人員的監督下界定其他角色。該等角色需執行與本文件其他條文符合的特定功能。在可能的情況下，所有對系統完整性有潛在影響的運作應須採取適當的責任分工。

6.3 人事保安管制

本部分列明對於核證機關人員聘用、監察、評核、培訓及終止僱用的管制。具體事項包括：

- 聘用程序，包括就招聘獲信任人士及其他執行敏感程度較低的職位的人士所進行的背景調查程序；

- 培訓要求及培訓程序，包括任何再培訓期限及再培訓程序；

- 不同角色之間職務輪換的次數及次序；

- 對擅自行動、不適當使用權力及擅自使用核證機關系統的僱員採取的評核基準及紀律處分和終止僱用程序；

- 管制透過合約聘用的人員，包括規定合約人員就其引致損失的行動需負責的賠償，監察合約人員的表現等；及

- 爲僱員提供的文件，如使用者手冊、操作程序等，以支援該等人員執行職務。

7 技術保安管制

本部分界定核證機關所採取的技術保安措施，以具體保障其已加密的密碼匙及啓動資料(如個人辨認密碼、密碼等)。核證機關須說明其希望對儲存庫或登記人等採取的任何要求或限制，以確保其加密密碼匙及重要的保安範圍得到適當的保障。穩妥的密碼匙管理對維持穩當系統產生決定性作用，核證機關須確保所有私人密碼匙及啓用資料得以保護並只由獲授權人士使用。本部分說明核證機關所採用的其他技術上的保安管制，以支援密碼匙及證書管理的運作。

核證機關所作出的管制必須與其他方面所作出的監控分開，例如任何以外發形式執行的功能(如註冊功能、儲存庫等)及登記人，以清楚界定有關方面的責任。

受管制的範圍包括：

- 配對密碼匙的產生、安裝，及管理其他方面的管理，包括：
  - 產生私人及公開配對密碼匙的責任；
  - 把私人密碼匙穩妥地送交登記人；
  - 把登記人的公開密碼匙穩妥地送交證書發出人；
  - 把核證機關的公開密碼匙穩妥地送交登記人；
  - 所採用的密碼匙大小及可用的技術；
  - 管制公開密碼匙參數的生產及品質檢查；
  - 產生密碼匙硬件或軟件模組；及
  - 密碼匙的使用及目的 (及爲 X.509 第三版本證書在密碼匙使用指示版上作出標示)。
- 私人密碼匙的保護，例如：
  - 密碼匙生產工具所需的標準(如適用)，例如密碼匙生產工具能符合國際標準化組織(ISO)訂立的 15782-1/ FIPS140-1 標準；
  - 就私人密碼匙使用多人控制；
  - 進行私人密碼匙的備份，包括備份的形式及有關備份系統的保安管制；
  - 私人密碼匙存檔，包括存檔密碼匙的形式及有關存檔系統的保安控制；
  - 對私人密碼匙啓動、使用及停止啓動的管制，包括如密碼匙數據輸入所需的人數、私人密碼匙的形式、啓動機制、已啓動的密碼匙的啓動期等；
  - 管制銷毀密碼匙，包括交出權標、毀滅權標或重寫密碼匙；
  - 公開密碼匙存檔；及

- 公開及私人密碼匙的使用期；

- 啓動資料的管制，其中列出啓動資料生命周期的管制，例如由產生、分派至存檔及銷毀。所考慮的管制措施與上段有關生產期配對密碼匙及保護私人密碼匙的內容類似；

- 電腦保安控制，其中列出爲防止及偵察核證機關系統在未經許可而擅自進入及修改或資料洩漏情況所採取的保安措施特徵。可參考有關的電腦保安架構，如 ISO 15408: 1999/ "The Common Criteria for Information Technology Security Evaluation (CC)；

- 管制系統發展生命周期，其中列出核證機關對系統發展生命周期所採取的管制措施，包括就初次配置核證機關設備所採購或發展軟件及硬件,以防止不正當干涉的程序；

- 網絡保安管制，其中列出保護核證機關設備所有接達的管制措施，例如適當設置及維持的防火牆，或相等的管制進入工具，及監控擅自進入的情況並防止遭受蓄意的攻擊；及

- 加密工具工程管制，其中列出加密工具的具體管制設施，可參考有關的標準，如 ISO15782-1/ FIPS140-1。

8 證書及證書撤銷清單結構

本部分列明核證機關所採用的證書格式及證書撤銷清單的格式，包括結構、版本及所使用的引述。核證機關一般會根據 X.509v3 證書格式(第三版本)的要求產生及管理公開密碼匙證書，並根據 ITUX.509v2 證書格式(第二版本)產生及刊登證書撤銷清單。

8.1 證書結構

本部分旨在爲證書結構的具體格式提供資料，涵蓋範圍可包括下列各項：

- 版本編號；

- 證書使所用的引述，特別是佔有重要位置的證書及其重要性；

- 加密算法的物件辨識項目;

- 所使用的名稱形式；

- 命名限制；
- 證書政策的物件辨識項目；
- 政策限制申延的使用；
- 政策鑑定字段的語法及語義；及
- 主要證書政策字段的語義處理。

8.2 證書撤銷清單結構

本部分旨在提供有關證書撤銷清單的資料，或令參考有關標準；包括：

- 證書撤銷清單的版本編號；及
- 證書撤銷清單及輸入證書撤銷清單資料申延的詳細資料及其重要性。須注意的是所採用的證書結構必須盡量簡單，以符合 RFC 2459 (Internet X.509 PKI Certificate and CRL Profile) 的標準。

9 規格釐定的行政

本部分指出如何備存核證作業準則。

9.1 規格釐定的變更程序

本部分指出對核證作業準則作出任何變更的程序，包括根據業務守則列出的規定通知署長、登記人及倚據人士有關的變更。核證機關須在核證作業準則的變更生效後盡快在儲存庫中公布。另外，核證機關亦可指明就某類型的變更不需要作出預先通知。

9.2 公布及通知程序

本部分列明核證機關在所有登記人及倚據人士知悉的儲存庫，該儲存庫可以是一個網址，公布所有有關資料的程序，並須指明該等儲存庫的位置及其他代替的資料來源。

10 互通性

爲促進互通性，核證機關可適當地選擇根據其所採用的技術指出其可支援的互通程度。核證機關爲此可能需要列明其系統所採用的特定標準或規約或其系統的組件。核證機關可公布的詳情包括其爲儲存庫採取的標準(如 LADP兼容)，或具體的證書資料(如 X.509)，證書申延等。

核證機關遵守規定的評估

引言

1 條例第 19(3)(b)條要求核證機關在申請認可時，必需向署長提交一份由一位經署長接納爲合資格的人所擬備的報告。該報告需載有對申請人是否有能力遵守條例適用於認可核證機關的條文的評估，及是否有能力遵守業務守則的評估。根據條例第 37(1)及(2)條，認可核證機關必須最少每 12 個月，向署長提交一份報告，而該報告須載有對該核證機關在所擬備的報告所涵蓋的期間內是否已遵守條例適用於認可核證機關的條文的評估，及是否已遵守業務守則的評估。此報告必須由署長認可爲合資格擬備該報告的人擬備。本附件對此等安排作進一步的闡明和解釋。

2 本附件旨在爲下列人士提供參考：

- 在條例第 19(3)條第(b)(ii)款及第 37(2)條所指的人，該人將擬備條例第 19(3)條第(b)(i)款及第 37(1)條所指的報告；
- 準備接受評估的核證機關；及
- 考慮申請認可的核證機關。

3 本附件分爲兩節。第一節列出合資格執行上述評估的人的基本資歷。第二節列出遵守規定的評估所涵蓋的基本範圍。

第一節：獨立評估人的資格

4 第一節的目的是就署長根據條例第 19(3)條(b)(ii)款及第37(2)條考慮接納爲合資格作出有關評估的人所應具備的資格提供指引。

評估人需

- 爲在組織上獨立於申請認可的核證機關的人士；及
- 爲認可專業機構或協會的合資格成員。該專業機構或協會亦需要求其成員遵從其規定，例如：
  - 持有特定的技能；
  - 遵守質素檢驗的規定，例如同業的監察 ；

- 成功完成由機構或協會所舉辦的能力測試；
- 遵守指派適當員工進行工作的標準；及
- 符合持續專業進修的要求。

■ 就以下各項具備可證明的技能：

- 公開密碼匙基礎建設及有關的科技，例如數碼簽署和證書等；
- 運用資訊保安工具及技能；
- 進行財務評估；
- 進行保安評估；及
- 進行第三者評估。

5 評估人是一個本身具備上述所有要求的人士，或是一個組織或機構，而其成員整體上須具備上述所有要求。簽署評估報告的人必須：

■ 是認可專業機構或協會的註冊會員，即是持有有效的執業證書或具備同等的資格；

■ 承擔整體責任以確保進行評估程序的人員具有在數碼簽署和證書、公開密碼匙基礎建設、財務事項等各方面足夠的知識；及

■ 承擔整體責任去確保評估的質素及評估的過程符合爲此等評估所訂下的標準及作業方法。

第二節：遵守規定的評估的範圍指引

6 第二節的目的是爲條例第 19(3)條第(b)(ii)款及第 37(2)條指定的評估的範圍及覆蓋面作出指引。

遵守規定的評估的目的

7 遵守規定的評估的目的是爲要確定：

■ 被評估的核證機關，從所有實質方面而言，是否能夠或一直能夠遵守條例有關條文的規定及業務守則；及

- 被評估的核證機關，從所有實質方面而言，有否遵守它在核證作業準則內所列明的政策及作業方法。

遵守規定的評估的範圍

8 此評估須根據條例所訂明的認可條件去處理核證機關所作出的有關聲明。評估的焦點在於該核證機關是否有能力遵守或已遵守條例的有關條文及業務守則。

9 評估的主要範圍會在以下各段闡明，最少應包括：

- 瞭解核證機關的政策及商業運作方式，並評估這些資料是否已作出正當披露；
- 評估該核證機關有否履行其財務上所作出的承諾，如承擔其債務；
- 評估該核證機關有否遵照有關使用穩當系統以支援其運作的要求；及
- 評估該核證機關有否遵照給予證書認可所作出的規定(如適用)。

核證機關政策及商業運作方式的披露

10 評估人員應取得並瞭解該核證機關所訂定的政策及商業運作方法。這些政策和方法的資料，包括該核證機關所提供或會提供的服務的細節，應載列在該核證機關所發出及備存的核證作業準則內。

11 若該核證機關有一個或多個證書政策，評估人亦需瞭解每一個政策內所載列出的規定。

12 評估人必須評估這些政策及商業運作方法是否根據條例及業務守則的規定作出披露。

評估財務承擔

13 評估人需評估該受評估認可核證機關在實質上是否有能力成爲和會保持爲有經濟能力的商業個體，並可持續運作。以下各方面須在考慮之列：

(a) 核證機關在決定其可能承擔的責任範圍時所採取的措施，包括確定有否爲可能因核證機關的職員、員工或代理的過失或失責而引起的賠償問題作出足夠的保障；例如爲失責購買專業彌償保險；

(b) 核證機關爲保障其履行發出的或計劃發出的證書內的倚據限額可能產生的法律責任所作的安排，例如核證機關備有適當的保險安排；及

(c) 核證機關意圖和會保持持續經營。此意圖可以多種方式表明，包括

- 維持足夠財務安排以支持其運作；

- 已裝置或準備裝置核證機關運作時所需要的系統及設備及作出所需的財務安排；及

- 無論是在質素(以技能而言)及數目(以人數而言)方面已僱用足夠的員工，以支持核證機關運作。

評估系統、程序保安上的安排和標準

14 條例第 31 條及業務守則規定認可核證機關在提供服務時必需使用穩當系統。被評估的核證機關需證明所使用的系統符合此規定及符合其核證作業準則的要求。認可核證機關業務守則的第五節列出評估穩當系統的指引。

15 評估人在作出評估的時候，應制訂適當的測試以爲確定核證機關在安裝及使用穩當系統方面提供足夠證據。

評估證書的延續循環控制

16 核證機關在申請認可某一類別的證書時需顯示：

(a) 證書是根據該核證機關的核證作業準則，及依照業務守則的規定發出；及

(b) 該核證機關爲保障其能履行其法律上的責任的賠償保險安排須與其業務相符。

17 評估人應取得足夠的證據，以便能從該核證機關所履行控制證書的延續性的有效程度來評估它能否符合以上各種情況。

報告

18 評估人須擬備一份關於評估結果和發現的正式書面報告。

19 評估人必須從各方面實質上評估有關核證機關，是否有能力或一直已遵守條例的有關條文及業務守則。評估人必須考慮下列各方面：

- 該核證機關有否在核證作業準則內披露其商業運作方式，而且有效地管理其作業準則及依照其所披露的商業運作方式提供服務。
- 該核證機關有否有效地管制及提供合理的保證，確保對其運作的環境控制可以符合維持一個穩當系統的規定；及
- 該核證機關有否有效地管制及提供合理保證，確保其核證機關的特定運作方式，包括密碼匙的管理和證書的延續性管理，能有效地遵照該核證機關的核證作業準則的規定。

採用內部審計工作

20 評估人員在適當的情況下需考慮採用核證機關內部審計工作的範圍，以修訂測試工作的性質、時間性及程度。如計劃採用內部審計工作，評估人需考慮：

- 內部審計工作的效能和目的；
- 內部審計工作涵蓋有關特定核證工作的範圍；及
- 就發現的問題作出跟進和解決這些問題的進度。

評估的操守

21 評估人需依照其所屬的專業機構或協會就進行評估工作所訂的標準及守則(如適用)，進行有關的評估工作。

22 評估人需根據各方面的評估結果，評定任何明顯的不遵守規定及不足之處的嚴重性。除評估報告外，評估人可與該核證機關就重要的發現聯絡，以加速改善其運作。

23 評估人需設計及進行測試以核實核證作業準則所訂立及與作業準則相關的核證政策的條文，是否已在其運作、技術及/或文件中作出充分反映。評估人員所作的測試應包括：

- 諮詢管理層及觀察該核證機關的運作；
- 查閱有關的文件及紀錄；
- 核對系統的設定安排；及
- 評估人認爲適當的其他測試。

24 除了上述問題外，評估人員亦需運用其專業的判斷力來決定在評估時所使用的測試程序的性質、時間性和程度。

參考及權威機構

25 就遵守規定進行評估時，評估人必須考慮適用於核證機關運作的一般已被接納的監控原則。在這方面現有的資料包括：

- Institute of Internal Auditors' Systems Auditability and Control Report
- Information Systems Audit and Control Association and Foundation, Control Objectives for Information and Related Technology (CObIT)
- ANSI (American National Standards Institute) ASC draft X9.79 standard, PKI Policies and Practices Framework, which includes the Certificate Authority Control Objectives in a normative annex
- AICPA/CICA CATrust Principles and Criteria
- Evaluation Criteria for Information Technology Security (Common Criteria)
- IETF PKIX Drafts and Requests for Comment