認可核證機關
業務守則

由政府資訊科技總監根據
《電子交易條例》（第 553 章）
第 33 條刊登

二零零四年十二月公布
(第二．一版)

香港特別行政區政府
政府資訊科技總監辦公室

本文件的版權屬香港特別行政區政府所有，
未經香港特別行政區政府明確批准
不得翻印其全部或其中任何部分內容。

修訂史				
更改編號	修訂說明	受影響的頁數	版本編號	日期
1.	第二版至第二．一版的更新如下： • 修改第 1.9 段以反映版本編號的更新 • 因應《2004 年專業會計師(修訂)條例》而修改第 12.4(a)段	 1 28	二．一	2004 年 12 月

目錄

1.	引言	1
2.	用語定義	1
3.	認可核證機關的一般責任	6
4.	核證作業準則	8
5.	穩當系統	9
	-通用釋義	9
	-指導原則	10
	-須予以考慮的特定範圍	10
	-行業內廣泛接受的的良好作業實務	10
	-認可核證機關特定功能的良好作業實務	15
	-使用穩當系統產生密碼匙及保存紀錄	18
	-數碼簽署	19
	-對穩當系統構成影響的事宜	19
	-保安及風險管理	19
6.	證書及認可證書	20
	-發出證書	20
	-暫時吊銷及撤銷認可證書	21
	-認可證書的續期	22
7.	登記人身分的核實	22
8.	倚據限額以及爲法律責任投保	22
9.	儲存庫	23
10.	披露資訊	24
11.	終止服務	25
12.	對遵守條例及本業務守則的評估	26
13.	聲明遵守條例及本業務守則的規定	29
14.	標準及技術的採用	29
15.	互通性	30
16.	消費者的保障	30

附錄 1 有關核證作業準則內容的標準及程序

附錄 2 就核證機關的評估而指明的《電子交易條例》及本業務守則的條文

1 引言

1.1 認可核證機關業務守則(“業務守則”)是政府資訊科技總監(“總監”)根據《電子交易條例》(第 553 章)(“條例”)第 33 條刊登的。

1.2 本業務守則指明認可核證機關在執行其功能時須採用的標準及程序。本業務守則應與條例一併閱讀。

1.3 總監根據條例第 21 條決定某申請人是否適合認可爲認可核證機關時，須考慮該申請人是否有能力遵守本業務守則。

1.4 總監根據條例第 22 條對個別證書或某類型、類別或種類的證書批給認可時，須考慮該個別證書或該類型、類別或種類的證書是否或會否由某認可核證機關按照本業務守則發出。

1.5 總監根據條例第 22、23、24 或 27 條可考慮因某認可核證機關未能遵守本業務守則而暫時吊銷或撤銷以下認可或不將其續期：批給該核證機關的認可，或對由該認可核證機關發出或擬發出的個別證書或某類型、類別或種類證書批給的認可(視乎屬何種情況而定)。

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 總監會不時對本業務守則作出修訂，並可就日後的修訂項目諮詢業界(包括根據條例第 21 及 34 條認可的核證機關）。諮詢業界的主要渠道是透過認可核證機關業務守則諮詢委員會。該委員會由總監擔任主席。

1.8 本業務守則的中文與英文版本之間如出現差異而引起任何衝突，須以英文版本爲準。

1.9 業務守則第二．一版取代 2004 年 7 月出版的業務守則第二版。

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：

(a) 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；

(b) 識別發出紀錄的核證機關；

(c) 指名或識別獲發給紀錄的人；

(d) 包含該獲發給紀錄的人的公開密碼匙；並且

(e) 由發出紀錄的核證機關簽署；

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	指由核證機關發出的證書或向核證機關發出的證書，用以證明該機關所發出的證書。該證書可以是核證機關發給本身的證書，或是某核證機關發給另一核證機關的證書；
核證機關披露紀錄	就任何認可核證機關而言，指根據條例第 31 條爲該機關備存的紀錄；
證書政策	指一套訂明的規則，表明證書對特定群體及／或有共同保安規定的使用類別的適用性；
核證作業準則	指認可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：

(a) 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

(b) 在產生數據變換之後，該原本的電子紀錄是否未經變更；

電子紀錄　指資訊系統所產生的數碼形式的紀錄，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；並且

(b) 能儲存在資訊系統或其他媒介內；

適當人選　在決定某人是否適當人選時，總監除考慮其認爲有關的任何其他事宜外，還須考慮是否有以下情況：

(a) 該人曾在香港特別行政區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；

(b) 該人曾被裁定犯本條例所訂的罪行；

(c) 如該人是個人，該人是未獲解除破產的破產人，或在先前 5 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

(d) 如該人是一間公司，該公司正在清盤中，或是清盤令的標的，或有接管人就該公司而獲委任，或該公司在先前 5 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　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的系統：

(a) 處理資訊的；

(b) 記錄資訊的；

(c) 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

(d) 能用作檢索資訊的（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　就某證書而言，指：

(a) 製造該證書，繼而通知在該證書內指名或識別爲獲發給該證書的人，關於該證書內所載與該人有關的資訊；或

(b) 通知將會在該證書內指名或識別爲獲發給該證書的人，關於將會在該證書內所載與該人有關的資訊，繼而製造該證書，

再繼而提供該證書，供該人使用；

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；

個人資料　指《個人資料（私隱）條例》（第 486 章）所界定的個人資料；

郵政署署長　指《郵政署條例》(第 98 章)所指的署長；

獲適當授權人　指獲授予權力代表登記人行事的人；

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	指下述證書：
	(a) 根據條例第22條認可的證書；
	(b) 屬根據條例第22條認可的證書的類型、類別或種類的證書；或
	(c) 郵政署署長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21條認可的核證機關，或郵政署署長；
紀錄	指在有形媒介上註記、儲存或以其他方式固定的資訊，亦指儲存在電子或其他媒介的可藉可理解形式還原的資訊；
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；
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；
簽及簽署	包括由意圖是認證或承認紀錄的人簽立或採用的任何符號，或該人使用或採用的任何方法或程序；
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）：
	(a) 在某證書內指名或識別爲獲發給證書；
	(b) 已接受該證書；及
	(c) 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：

(a) 是合理地安全可免遭受入侵及不當使用的；

(b) 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；

(c) 合理地適合執行其原定功能；及

(d) 依循獲廣泛接受的安全原則；

核實數碼簽署　就某數碼簽署、電子紀錄及公開密碼匙而言，指確定：

(a) 該數碼簽署是否用與列於某證書內的公開密碼匙對應的私人密碼匙而產生的；及

(b) 該電子紀錄在其數碼簽署產生後是否未經變更，

而凡提述數碼簽署屬可核實者，須據此解釋。

3 認可核證機關的一般責任

3.1 認可核證機關須遵守總監根據條例第 21 條批給認可時附加的條件，或根據條例第 27 條將認可續期時附加的條件。

3.2 認可核證機關可委任代理人或分包商執行其部分或所有運作，但須符合下列條件：

- 該代理人或分包商應具備同等能力以遵守本業務守則內適用於其運作的規定；及
- 認可核證機關須由始至終對其代理人或分包商所執行或其本意是執行條例就該機關規定的功能、權力、權利和職責負責。

3.3 認可核證機關在向其登記人發出證書時，須在合理範圍內盡量小心，及須在合理範圍內盡量小心處理可能倚據由該機關發出的證書的人。

3.4 認可核證機關須向總監提供其用以簽署認可證書的核證機關證書。總監須在爲該機關備存的核證機關披露紀錄內公布該核證機關證書。有關的披露紀錄可在該機關終止服務後的最少 7 年內，提供額外途徑，使有需要核實由該機關發出的認可證書有效性的人，可取得有關的證書。

3.5 凡本業務守則規定認可核證機關把資訊及紀錄加以記錄、保留或存檔，該機關須把該等資訊及紀錄記錄、保留或存檔爲期最少 7 年，或由總監指明的較長或較短的期間，並須以能確保該等資訊及紀錄的安全、完整及可供接達的方式處理，以便檢索和查閱。

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及規例。認可核證機關尤須：

(a) 列明其有關以下事項的私隱政策：資料當事人（例如證書申請人及登記人）的個人資料的收集、持有和使用；

(b) 在向資料當事人收集個人資料之前或之時，向資料當事人發出一項書面的收集個人資料聲明；

(c) 包括一項目的聲明（例如在其儲存庫或核證作業準則內），闡明保存其儲存庫的目的，以及儲存庫內所載個人資料的許可用途；及

(d) （作爲一項最低限度的規定）按照個人資料私隱專員出版的《遵守〈個人資料（私隱）條例〉規定自我評估資料套》或同類性質的文件進行自我評估，以確保與個人資料私隱有關的所有適用條例和規例得以遵守。認可核證機關須定期或每當其運作發生重大變化以致影響其處理資料當事人的個人資料時，進行此類自我評估。

3.7 認可核證機關不得使用任何有損經濟效益或自由貿易的限制性作業實務。

3.8 如認可核證機關向公眾發出的證書中有認可的證書和非認可的證書，該機關須在其核證作業準則和儲存庫中公布其發出該兩種不同類目的證書的事實。該機關如此公布事實時，須清楚識別其所發出的個別證書或某類型、類別或種類的證書中何者屬根據條例獲認可的證書而何者屬非認可的證書。

3.9 認可核證機關須按照有關防止對殘疾人士施行歧視性的做法的所有條例和規例，在提供服務時顧及殘疾人士的需要。

4 核證作業準則

4.1 認可核證機關須就其發出的各類型、類別或種類的認可證書，向公眾公布及備存其最新的核證作業準則。

4.2 認可核證機關須在其核證作業準則內述明該機關、其登記人及倚據其發出的證書的人的法律責任、法律責任限額、權利和責任，以及該機關在其證書內設定的倚據限額的重要性。認可核證機關須透過以下方法，使其登記人及倚據該機關發出的證書的人注意到該等法律責任、法律責任限額、權利和責任及倚據限額的重要性：

- 在與登記人訂立的任何合約內適當地另行指明該等資訊；及
- 以書面及聯機的和可供公眾接達的電子媒介提供該等資訊。

4.3 認可核證機關須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，提供最新的資訊。

4.4 認可核證機關須令其登記人及可能倚據其發出的非認可的證書的人，知悉使用及倚據該等證書的影響。

4.5 認可核證機關須令其證書的申請人知悉，當該機關把申請人的個人資料納入在向申請人發出的認可證書，及把該證書在該機關的儲存庫公布時，該等資料便會成爲公開資訊的程度。該機關的核證作業準則必須明確述明有關的認可證書的內容。

4.6 認可核證機關須在公布核證作業準則後，向總監提交該準則的副本，並於切實可行範圍內盡快以書面通知總監其後有關該準則的任何變更。認可核證機關亦須於切實可行範圍內盡快記錄該準則的所有變更及每項變更的生效日期。

4.7 如認可核證機關發出已在某證書政策指明的某類型、類別或種類的認可證書，該證書政策會當作核證作業準則的一部分。

4.8 認可核證機關須保留其核證作業準則每個版本的副本，並須列明核證作業準則的生效日期及停止生效日期（如適用）。

4.9 認可核證機關在發出某類型、類別或種類的認可證書時，須遵守關於該類型、類別或種類的認可證書的核證作業準則。

4.10 認可核證機關須確保其核證作業準則可隨時在聯機的及可供公眾接達的儲存庫內查閱。核證作業準則有任何變更時，儲存庫內的資訊須盡快予以更新。

4.11 有關核證作業準則內容的標準及程序載於附錄 1。

4.12 認可核證機關擬對其運作或與該機關發出的一個或多個類型、類別或種類的認可證書對應的核證作業準則作出重大變更前，須以書面通知總監有關變更的詳情。總監將會考慮該機關擬作出的重大變更是否符合條例及本業務守則的有關條文，並可要求該機關按照第 12.1(c)及 13.1(c)段向總監呈交有關重大變更的報告及/或法定聲明。認可核證機關的運作方面或其核證作業準則的重大變更包括但不限於以下例子：

(a) 會減低認可證書可靠性的有關識別程序的變更；

(b) 認可證書的依據限額的變更；或

(c) 密碼匙的產生、儲存或使用程序的變更。

4.13 凡有任何事件會不利於及嚴重影響其核證作業準則的全部或部分有效性，認可核證機關須立即通知總監、登記人及倚據人士。該機關須立即處理該事件。該等事件的解決辦法須在切實可行的範圍下，盡快在核證作業準則內反映、在該機關的聯機的儲存庫公布及向總監報告。

5 穩當系統

5.1 認可核證機關須使用穩當系統提供服務，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訊。

通用釋義

5.2 “系統”一詞指系統本身，即硬件和軟件，及管制和運作程序（人手及自動操作的程序）。制訂有關程序旨在確保該系統能一致、可信及可靠地執行其原定的功能。

5.3 認可核證機關須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原定的功能，系統才可獲接受爲穩當系統。

5.4 量度穩當程度並無一套絕對的標準。穩當程度只能以某一個特定的情況作出評估。

指導原則

5.5 在條例所採取的科技中立及盡量少加規管的原則下，認可核證機關可自行選擇支援其運作的技術方案。

5.6 凡認可核證機關有部分運作範圍（如與影響保安的功能有關的運作）具高風險，該機關所採用的系統及程序會被預期是可符合國際間廣泛接受或認可的標準。此外，就良好的作業實務而言，認可核證機關須就確定其運作的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。

須予以考慮的特定範圍

5.7 在公開密碼匙基礎建設下運作的認可核證機關，須應用硬件、軟件及密碼組件。這些組件須有適當的保安政策及程序作配合，以確保認可核證機關能在穩妥可靠的環境下運作。

5.8 認可核證機關爲達致保持系統穩當的目的所採用的方法，會因應不同認可核證機關提供的服務種類、科技狀況及業務環境而可能有所不同。認可核證機關須依循以下獲廣泛認可的良好作業實務。

行業內廣泛接受的良好作業實務

5.9 認可核證機關須就其營運環境發展、制訂、備存及更新有正式記錄及經核准的政策、程序及作業實務，其中包括但並不限於下文的討論範圍。

獲廣泛接受的保安原則

5.9.1 認可核證機關須根據獲廣泛接受的保安原則，就其運作發展、制訂、備存、更新及推行足夠及適當的保安管制措施。保安原則最少須涵蓋下列各項：

(a) 資產分類及管理

(i) 認可核證機關須把其資產按適當的方式分類，並爲其主要資產識別擁有人。該機關須備存最新及完整的資產清單，並制訂程序以保障其資產；

(ii) 認可核證機關須把所備存的資訊當爲其中一種資產，並根據業務運作的重要性（包括資料私隱的考慮因素）爲該等資訊分類。該機關須制訂適當的管制措施，以保證該等資訊不會被人擅自接達或破壞。

(b) 人事保安

(i) 認可核證機關須透過多種機制發展、制訂、備存及更新有效的人事保安管制措施，其中包括但不限於：

- 根據其保安政策在正式的工作定義內對工作種類的職責及責任加以界定；
- 根據其保安政策及程序對其員工進行保安審核；及
- 在僱傭合約的正式條款及條件內納入保持機密性或類似的條款。

(ii) 認可核證機關須爲其職員提供適當及足夠的培訓，目的是維持他們執行任務的能力，以確保保安政策得以有效推行和予以遵守。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
- 處理保安事件及通知高層管理人員有關重大保安事件的程序。

(iii) 認可核證機關須制訂適當的管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。

(c) 實體及環境保安

(i) 認可核證機關須執行有效的實體及環境保安管制措施，其中包括但不限於：

- 識別及界定保安範圍，並採取適當的保安管制措施以確保該等範圍的安全；
- 就認可核證機關的職員及訪客進入該等範圍制訂正式的程序；

- 設立適當的保安及進入保安範圍的監察機制，而認可核證機關用以儲存影響保安的設備的範圍須特別加以注意；

- 制訂適當的管制措施，以保障其設備免受火災、水災、停電等環境因素及災患影響，並須防止有人擅自進入保安範圍內；

- 制訂一般的保安管制措施，例如：清理桌面政策及對屬於認可核證機關的設備、資訊及其他資產的一般管制；及

- 確保其環境管制機制得以維持，並按時進行檢討。

(ii) 凡認可核證機關倚靠第三方提供服務，以保障實體及環境的保安，該等服務須在該機關與第三方供應商訂立的正式服務協議內述明。

(d) 系統接達的管理

認可核證機關須就其資訊系統（包括應用系統）的接達發展、制訂、維持及更新有效的管制措施及程序。該等管制措施及程序須因應受保護系統的敏感性及關鍵性而發展、制訂、維持及更新，其中包括但不限於：

- 制訂適當的業務規定以管制系統的接達；

- 正式釐定用戶的責任；

- 就用戶識別資料管理及系統接達的監察制訂正式程序，其中包括：

  － 分配、修改及撤銷用戶的接達權；及

  － 利用記錄或類似方法監察嘗試接達系統的情況；

- 就接達網絡、操作系統及應用系統制訂適當的管制措施，如防火牆和路由器篩選指令；

- 就監察系統接達及使用制訂適當的程序及管制措施；

- 就流動電腦應用及電訊運作制訂適當的程序及管制措施；

- 就擅自或非法使用軟件制訂適當的程序及管制措施；及

- 就與接達網絡、操作系統及應用系統有關的保安事件制訂適當的處理程序。

操作管理

5.9.2 認可核證機關須就其日常的操作維持有效的管制措施及程序。操作政策及標準操作程序須予以正式制訂及記錄，其中包括但不限於以下範圍：

- 清楚界定其操作人員的職務及責任；

- 制訂定期監察系統承擔能力的程序，以監察系統的工作表現及找出窒礙系統工作表現的地方；

- 制訂適當的程序，以防止其電腦基建設施受有害程式（如電腦病毒等）的影響；

- 制訂適當的系統及網絡管理程序，包括備份及存檔等內務管理；

- 就電子資訊及媒體的處理、分發、儲存及處置制訂適當的程序；及

- 制訂適當的程序處理及解決操作上的問題。

電腦系統的發展及維修保養

5.9.3 認可核證機關須就系統的發展及維修保養工作發展、制訂、維持及更新有效的管制措施及程序，其中包括：

- 制訂適當的內部標準，以確保無論由認可核證機關的人員或在外發的情況下由外間機構進行發展工作時，均能保持一貫的標準；

- 制訂程序，以確保把用作生產及發展的環境分隔開；

- 制訂程序，以確保操作及發展人員的職責得以區分；

- 對接達其用作生產及發展的環境內的資料及系統制訂管制措施；

- 對變更管制程序（包括系統及／或數據的緊急變更）制訂管制措施；及

- 就採購設備及服務的妥善管理制訂程序。

業務運作的持續性

5.9.4 認可核證機關須發展、制訂、維持及更新涵蓋所有關鍵的運作範圍的業務持續運作計劃。

5.9.5 該持續運作計劃須定期進行徹底的測試，而計劃所載列的有關主要人員須參與進行測試。在可能範圍內，須聘用獨立人士觀察這些測試的進行。

5.9.6 業務持續運作計劃須涵蓋緊急應變措施，例如：認可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後的復原運作，或認可核證機關的系統或其系統的任何組成部分出現重大故障後的復原運作。

備存適當的事件紀錄

5.9.7 認可核證機關須備存足夠的事件紀錄，包括保留與該機關發出及管理認可證書有關的文件。

5.9.8 認可核證機關須爲該等事件紀錄存檔。該機關亦須定期檢查事件紀錄，並就經識別的任何異常情況採取行動。

5.9.9 認可核證機關須爲所有重大事件備存紀錄，其中包括但並不限於：

- 對用以產生密碼匙的資料及設備的接達；
- 密碼匙及證書及其產生、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；
- 保安事件，包括密碼匙資料外洩；及
- 密碼設備的採購、安裝、使用、解除運作及棄用。

對遵守規定的監察及保證

5.9.10 認可核證機關須發展、制訂、維持及更新適當的管制措施，以確保能遵守適用的法律、規管及技術方面的規定，其中包括但不限於：

- 制訂適當的功能，以監察認可核證機關的所有運作程序，並確保遵守所適用的規定；

- 確保其遵守監察的功能符合業界的現行標準及作業實務；及

- 就操作系統安排進行適當的檢討。

認可核證機關特定功能的良好作業實務

5.10 認可核證機關需就其特定的功能發展、制訂、維持及更新有正式記錄及經核准的政策、程序及作業實務，其中包括但不限於下文所載的範圍。

核證作業準則的管理

5.10.1 認可核證機關須在核證作業準則內披露業務的作業實務，並對核證作業準則執行有效的管制措施，其中包括但不限於：

- 成立管理小組，並授予制訂及核准核證作業準則的權力及責任，包括認可核證機關所採用的任何證書政策；

- 制訂有效程序，以持續檢討及更新核證作業準則；及

- 使核證作業準則可供登記人及可能倚據由該機關發出的認可證書的人查閱。

監察認可核證機關的功能以確保其遵守法律和規管

5.10.2 認可核證機關須維持有效程序，以監察及確保其遵守所有法律及規管方面的規定，包括條例有關的條文、根據條例訂立的規例及本業務守則。

密碼匙的管理

5.10.3 認可核證機關須就該機關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管制措施，其中包括但不限於：

- 有關使用產生密碼匙的密碼模組的管制措施，包括採用符合適當保安標準的技術方案;

- 有關產生密碼匙的操作管制措施，其中包括但不限於：

  – 用以確保用於產生密碼匙的設備完整無誤的程序；及

  – 用以確保密碼匙是由獲授權人在受管制的方式下產生的程序；

- 有關密碼匙的儲存、備份及復原的管制措施，其中包括但不限於：

  – 認可核證機關的運作復原程序的定期徹底測試；

  – 用以確保核證機關的私人密碼匙得以安全地保管的程序，例如：採用雙重接達的保管方法。認可核證機關須制訂適當的措施，以確保能偵測任何嘗試擅自接達該機關的私人密碼匙的情況；及

  – 用以確保認可核證機關的私人密碼匙的備份得以在雙重接達的管制下安全地運作的程序，及該機關的私人密碼匙的備份應以穩妥的方式保管；

- 有關分發密碼匙程序的保安管制措施，其中包括但不限於：

  – 用以確保認可核證機關提供予總監在其核證機關披露紀錄內存放的公開密碼匙是完整及真確的程序；及

  – 用以確保認可核證機關本身的公開密碼匙是完整及真確的程序；

- 有關使用密碼匙的管制措施，包括啓動密碼匙的程序，例子包括但不限於：

  – 須有一名以上的負責人員才可啓動認可核證機關的私人密碼匙；及

  – 只有在取得適當的授權經訂明的方式以進行原定目的，才可啓動認可核證機關的私人密碼匙；

- 有關確保安全銷毀配對密碼匙及任何有關設施的管制措施，包括採取程序以確保銷毀私人密碼匙的所有副本（令私人密碼匙在銷毀後再不能復原或重組），以及撤銷對應的公開密碼匙的程序；及

- 有關確保已存檔的密碼匙符合在核證作業準則內述明的保安及運作規定的管制措施。

產生密碼匙工具的管理

5.10.4 認可核證機關須就產生密碼匙工具的採購、接收、安裝、驗收測試、調試、使用、維修、保養及棄用，維持有效的程序及管制措施，例如：

- 維持程序，以確保密碼模組的完整性；

- 維持程序，以確保產生密碼匙的工具由獲授權人在適當的督導下操作，以防止工具遭擅自改動；並設立管制機制，以確保密碼模組不會在不能偵測的情況下遭人擅自改動；及

- 維持程序，以確保使用密碼模組產生的密碼匙的強度，是符合認可核證機關及登記人爲密碼匙的目的所需的適合強度。

由認可核證機關提供的密碼匙管理服務（凡適用）

5.10.5 如認可核證機關爲登記人提供密碼匙管理服務，便須就密碼匙的產生、儲存、備份、復原、銷毀、及存檔等方面，執行有效的程序及管制措施。該等程序及管制措施須符合載於本業務守則第 5.10.3 及 5.10.4 段的原則。凡登記人的配對密碼匙由認可核證機關產生，該機關須制訂程序，以確保私人密碼匙以安全的方式及在沒有被擅自改動的情況下交付證書申請人；認可核證機關倘沒有登記人的書面同意，不得備存登記人的私人密碼匙副本。

權標的生命周期管理（凡適用）

5.10.6 認可核證機關須就其所使用的任何權標（如智能卡）的預備、啓動、使用、分派及終止使用，維持有效的程序及管制措施。

證書管理

5.10.7 認可核證機關須就證書的管理，維持有效的程序及管制措施，其中包括但不限於下列例子：

- 認可核證機關須根據有關的核證作業準則所載列的程序，核實申請發出證書或將證書續期的人的身分。該機關亦須核實該人的特有名稱的獨特性；

- 認可核證機關須訂立適當程序，使其在登記人的證書的有效期屆滿前，通知登記人須爲證書續期；

- 認可核證機關須採取開放及共通的界面以發出認可證書，而證書的格式須在有關的核證作業準則內述明；

- 認可核證機關須制訂適當的政策及程序，以確保該機關的儲存庫的效能，符合該機關在核證作業準則內就儲存庫所載列的服務水平；及

- 認可核證機關須在核證作業準則內載列處理登記人投訴的程序。

證書撤銷資訊公布的管理

5.10.8 認可核證機關須就證書撤銷資訊公布的管理（例如透過其證書撤銷清單及任何其他公布有關證書撤銷資訊的方式），制訂有效的程序及管制措施，例如：

- 認可核證機關須按照在核證作業準則內述明的政策、程序及安排，更新證書撤銷清單及任何其他公布有關證書撤銷資訊的方式；及

- 認可核證機關須制訂程序，以確保只有獲授權人才可接達儲存庫、證書撤銷清單及任何其他公布有關證書撤銷資訊的方式，以進行修訂的工作。

使用穩當系統產生密碼匙及保存紀錄

5.11 認可核證機關須使用穩當系統爲本身及登記人產生配對密碼匙。凡其任何認可證書的申請人使用自己的系統產生其配對密碼匙，認可核證機關須要求該申請人使用穩當系統以產生其配對密碼匙。認可核證機關須向申請人提供指引，並須採取合理地切實可行的措施，以確定申請人在使用穩當系統以產生其配對密碼匙方面遵守指引。如該申請人沒有遵守指引或沒有使用穩當系統以產生配對密碼匙，認可核證機關不得接受該申請人的配對密碼匙。

5.12 認可核證機關須把本身的私人密碼匙及啓動數據（如個人識別密碼、密碼等）以安全的方式分開保存。

5.13 認可核證機關須製備及保留下列紀錄：

- 有關認可證書的發出、續期、暫時吊銷及撤銷的事項（包括向認可核證機關申請認可證書的任何人的身分證明文件）；

- 證書撤銷資訊的公布（例如透過證書撤銷清單及任何其他公布有關證書撤銷資訊的方式）；

- 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。

5.14 認可核證機關須爲其發出的所有認可證書存檔，並設置接達該等證書的機制。

數碼簽署

5.15 所推行的技術就產生數碼簽署方面須遵守的規定：

(a) 數碼簽署須在其有關的人的指示下才能產生；及

(b) 在與數碼簽署有關的人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產生有效的數碼簽署。

對穩當系統構成影響的事宜

5.16 若發生任何會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的事件時，該機關須：

- 立即把有關事件告知總監；
- 合理地盡力通知所有已經或將會受該事件影響的人；及
- 按照核證作業準則就處理該類事件所指明的程序（如有指明的話）採取行動。

5.17 認可核證機關須確保其所有人員具備所需知識、技術資格和專業知識，以便有效地履行職責。

5.18 認可核證機關須確保所有負責人員和擔當獲信任職位的人員，例如保安主任、核證機關行政主管、特別系統操作人員、登記人員、及其他能接達重要資料、密碼模組及工作事件紀錄的人員，均爲適當人選。

保安及風險管理

5.19 認可核證機關須採用按普遍接受的保安原則制訂的保安政策。

5.20 認可核證機關須就其運作，制訂全面的保安事件匯報和處理程序，以及運作復原的機制和程序。

5.21 認可核證機關須充分地識別及制訂程序，以處理與該機關的運作有關的風險。該機關須推行一套風險管理計劃，就管理包括但不限於以下的事件作出規定：

- 密碼匙資料外洩；
- 認可核證機關的系統或網絡出現違反保安事項；

- 認可核證機關的基建設施不可供使用的情況；及
- 擅自製造有關證書及證書的暫時吊銷和撤銷的資訊。

6 證書及認可證書

6.1 認可核證機關可發出認可證書或非認可的證書。如認可核證機關發出的證書中有認可證書及非認可的證書，該機關須以不同的私人密碼匙分別簽署這兩類證書。

6.2 認可證書內應載有所需資訊，以協助登記人及依據證書的人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 認可核證機關只有在以下情況才可發出認可證書：

(a) 該機關已收到申請人提出的發出認可證書的要求；及

(b) 該機關已遵守核證作業準則載列的所有作業實務及程序，包括與該類型、類別或種類的認可證書有關的申請人的身分核實程序。

6.4 認可核證機關須爲其任何認可證書的申請人提供合理機會，以核實已經或將會收納入證書內的申請人資訊。申請人資訊是指由申請人提供而認可核證機關已經或將會收納入證書內的資訊。此外，該機關必須採取一切合理地切實可行的措施，確保已經或將會收納入證書內的資訊準確無誤。

6.5 認可核證機關須在其設置的或由一個或多個第三方爲其設置的聯機的及可供公眾接達的儲存庫內，公布由該機關發出且獲登記人接受的認可證書。如認可核證機關向公眾發出的證書中有認可證書及非認可的證書，該機關須用獨立的儲存庫分別公布該兩類證書。

6.6 認可核證機關須得到認可證書申請人的同意，才可按該機關的原意把申請人的個人資料收納入該等將予發給申請人的證書內，並將該等證書載列於聯機的及可供公眾接達的儲存庫內。

6.7 認可證書經認可核證機關發出且獲登記人予以接受後，倘該機關知道有任何影響認可證書的有效性及可靠性的事實，便須在一段合理時間內，透過所有渠道把該事實通知登記人。

6.8 認可證書須述明其有效性屆滿的日期。

6.9 凡認可核證機關發出認可證書，即屬向任何合理地倚據該證書的人，或向任何合理地倚據該證書內列出的公開密碼匙所能核實的數碼簽署的人，表述該機關已按照適用的核證作業準則發出該證書。

6.10 所有與發出認可證書有關的交易事項，包括日期和時間，均須予以記錄。

暫時吊銷及撤銷認可證書

6.11 認可核證機關可按下文載列的規定撤銷認可證書，亦可按該等規定暫時吊銷認可證書。

6.12 認可證書須包含或以提述方式收納所需資訊，以找出或識別載列與公布該證書的暫時吊銷或撤銷有關的通知的儲存庫。

6.13 除非認可核證機關及登記人另有協議，否則發出認可證書予登記人的認可核證機關須在接獲下列人士的要求後的一段合理時間內，暫時吊銷或撤銷該證書：

(a) 認可證書內指名或識別的登記人；或

(b) 獲適當授權人。

6.14 認可核證機關須於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外間機構代其設置的儲存庫內，公布有關暫時吊銷或撤銷認可證書的通知（例如透過認可核證機關簽署的證書撤銷清單，或任何其他公布有關暫時吊銷或撤銷認可證書的資訊的方式）。

6.15 認可核證機關撤銷或暫時吊銷證書的確實時間，以及由接獲撤銷或暫時吊銷認可證書的要求之時起至證書被撤銷或暫時吊銷之時止的一段期間，以該證書進行交易的法律責任攤分問題，須由認可核證機關和登記人議定。

6.16 如認可核證機關有合理理由相信其發出的某認可證書不可靠，則無論登記人同意與否，該機關可暫時吊銷該證書；但該機關須在一段合理時間內完成有關該證書的可靠性的調查，以及決定是否恢復該證書的有效性或撤銷該證書。

6.17 如認可核證機關在考慮所有可取得的資訊後，認爲應即時撤銷其發出的某認可證書，則無論登記人同意與否，該證書須予以撤銷。

6.18 如登記人或獲適當授權人要求暫時吊銷認可證書，認可核證機關須向該登記人或獲適當授權人查詢，該將會被暫時吊銷的認

可證書在暫時吊銷後是否須被撤銷或會否恢復該證書的有效性。有關的核證作業準則須述明該機關在未能聯絡該登記人或獲適當授權人時應採取的行動。聯絡有關人士的目的，是取得有關該證書在暫時吊銷後須予撤銷或恢復有效性的指示。

6.19 如認可核證機關暫時吊銷或撤銷所發出的認可證書，該機關須在一段合理時間內，把暫時吊銷或撤銷該證書之事，通知該證書的登記人或獲適當授權人，並向他們提供通知紀錄。

6.20 認可核證機關須提供熱線電話或其他設施，以供登記人向該機關報告有關影響其證書或私人密碼匙的事件，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所有交易事項，包括日期和時間，均須予以記錄。

認可證書的續期

6.22 認可證書可因應登記人的要求及認可核證機關的酌情權，在認可證書的有效期屆滿時獲得續期。

6.23 與認可證書續期有關的所有交易事項，包括日期和時間，均須予以記錄。

7 登記人身分的核實

7.1 認可核證機關須在與某類型、類別或種類的認可證書對應的有關核證作業準則內，指明對向該機關申請該等認可證書的人進行身分核實的程序。

7.2 認可核證機關須保留足以識別登記人身分的文件證據。

8 倚據限額以及爲法律責任投保

8.1 認可核證機關在向登記人發出某類型、類別或種類認可證書時，可在與該類型、類別或種類證書對應的有關核證作業準則內指明該等證書的倚據限額。該機關須在有關的核證作業準則指明倚據限額對使用該證書的重要性。

8.2 認可核證機關須安排投購適當的保險或作出其他方式的賠償安排，以確保該機關有足夠能力承擔因發出或使用認可證書而引起的或與此有關的潛在法律責任。該機關須特別提供證據，證

明本身已投購保險，承保因其錯誤或不作爲而引起的申索，而投保期內每宗申索的最低彌償額不得少於以下數額（以較高的數額爲準）：

(a) 該認可核證機關在其認可證書的核證作業準則上指明的倚據限額的 10 倍（如在一份保險單內就不同的認可證書指明不同的倚據限額，則採用當中最高的倚據限額）；或

(b) 港幣 200,000 元；

此外，該機關爲此目的而購買的每一份保險單在任何一段爲期 12 個月的投保期內，就該保險單所承保的認可證書的申索總額而設定的投保額，須爲上述(a)項或(b)項所述數額的 10 倍（以較高者爲準）。上述爲法律責任投購的保險必須在任何時候均有效，並須就該機關所發出的所有類型、類別或種類的認可證書提供保障。如該機關選擇以其他方式爲法律責任作出賠償安排，則所作出的安排必須提供相同的最低彌償額，並須由獨立的第三方加以管理。所作出的其他方式賠償安排生效之前，該機關必須先徵得總監批准。

8.3 認可核證機關所購買的保險單必須：

(a) 由根據《保險公司條例》（第 41 條）獲授權在香港特別行政區進行有關保險業務的保險人（包括勞合社）發出；及

(b) 受香港特別行政區的法律管限並按照該等法律解釋。

此外，認可核證機關及保險人均須同意就保險單所引起的申索或其他事宜受香港特別行政區法院的非專有司法管轄權所管轄。

8.4 對於因認可核證機關的錯誤或不作爲而引起的申索，該機關須維持一套程序規則，訂明提出申索時所需的證明文件。

9 儲存庫

9.1 認可核證機關須提供最少一個聯機的及可供公眾接達的儲存庫，以公布認可證書及其他有關的資訊。該機關須確保其一個或多個的儲存庫是由穩當系統所提供，並須在核證作業準則內述明有關儲存庫運作的服務水平。

9.2 認可核證機關在維持及管理儲存庫時，不得進行任何對倚據包含在儲存庫內的認可證書及其他資訊的人造成不合理風險的活動。

9.3 認可核證機關的儲存庫須載有：

- 由認可核證機關發出的認可證書；
- 有關暫時吊銷或撤銷認可證書的通知（包括證書撤銷清單，或任何其他公布有關暫時吊銷或撤銷認可證書的資訊的方式（視何者適用而定））；
- 該機關的核證機關披露紀錄；及
- 總監指明的其他資訊。

9.4 認可核證機關的儲存庫不得載有其明知爲不正確或不可靠的資訊。

9.5 認可核證機關須在其儲存庫內把過去最少 7 年內被暫時吊銷或撤銷的或有效期屆滿的認可證書存檔。

10 披露資訊

10.1 認可核證機關須在其一個或多個儲存庫內公布：

(a) 該機關的核證機關證書，其中包含與該機關用以在所發出認可證書作數碼簽署的私人密碼匙對應的公開密碼匙；

(b) 其核證機關證書或總監向其作出的認可被暫時吊銷、撤銷或不獲續期的通知；及

(c) 對該機關曾發出的認可證書的可靠性，或該機關提供與條例有關的服務的能力造成重大及不利影響的任何其他事實。

10.2 如認可核證機關在聘用負責人員或任何與負責人員有相同功能的人員方面有任何變更，須在該人員受聘日期起計 3 個工作日內把變更通知總監。

10.3 認可核證機關須每 6 個月一次，向總監提供包含以下資訊的進度報告：

(a) 按類型、類別或種類證書區分的登記人的數目；

(b) 按類型、類別或種類區分的發出、暫時吊銷、撤銷、有效期屆滿及獲得續期的證書數目；

(c) 服務表現與所述明的服務水平的比較；

(d) 所發出的新類型、類別或種類的證書；

(e) 組織結構或系統的變更；

(f) 認可核證機關所採取的行動，該等行動旨在處理根據條例第 20(3)(b)、第 27(5A)(b)、第 43(1)(a)及第 43A(1)(c)條所擬備及向總監提供的評估報告內所作出的建議或識別出的例外情況或不足之處；及

(g) 自上一次提供進度報告或申請認可爲認可核證機關或申請認可續期以來，以上各項目的任何變更情況。

10.4 以上各項資訊如有任何重大改變，認可核證機關須立即向總監報告。在有需要的情況下，總監亦可隨時給予一段合理時間的通知，要求該機關提供該等報告及其他與條例有關的資訊。

10.5 認可核證機關發現任何可能或將會導致與該機關的運作產生潛在利益衝突的事項時，須立即向總監報告。

10.6 認可核證機關須就任何可能對其運作構成重大及不利影響的事件，立即向總監報告。

10.7 認可核證機關根據條例及業務守則的規定提交任何報告或資訊時，須確保其本身對該等報告及資訊擁有所需的權力，以致能批予總監或促致他人批予總監特許，俾能爲施行條例而複製和發布該等報告和資訊的全部或其中任何部分內容。認可核證機關必須在總監提出要求時批予總監或促致他人批予總監該項特許。認可核證機關須因應總監的要求自費採取行動和簽立文件（或促致他人採取行動或簽立文件），以使該項特許有效。

10.8 認可核證機關同意讓總監披露上述報告及資訊，只要總監認爲爲施行條例而適宜披露便可。

10.9 認可核證機關不得企圖以任何方式阻止總監發布其爲施行條例而須發布的資訊。

11 終止服務

11.1 核證機關於申請成爲認可核證機關時，須向總監提交一份終止服務計劃。認可核證機關於申請將認可續期時，須提交一份最新的終止服務計劃。在總監提出要求時，該機關亦須在總監向該機關發出的通告中所指定的時間內，提交一份最新的終止服務計劃。

11.2 終止服務計劃須訂明關於認可核證機關終止服務的安排，尤其是把紀錄存檔最少 7 年的安排。該等紀錄包括該核證機關發出的證書以及該機關本身的核證機關證書。

11.3 終止服務計劃須涵蓋認可核證機關自願及非自願地終止服務兩種情況，當中包括總監對該機關作出的認可的有效期屆滿或認可被撤銷的情況。終止服務計劃亦須訂明有關措施，以確保登記人的利益在認可核證機關終止服務後仍能得到保障。

11.4 認可核證機關公布的任何核證作業準則均須提述該核證機關的終止服務計劃。

11.5 認可核證機關在終止運作前，必須：

(a) 在終止其核證服務前最少 90 日，把終止服務的意向告知總監；

(b) 在終止其核證服務前最少 60 日，把終止服務的意向告知其所有登記人；

(c) 在終止其核證服務前最少 60 日，在香港特別行區發行的一份英文報章及一份中文報章刊登有關擬終止服務的啓事最少連續 3 日；

(d) 在總監認爲有此需要時作出安排，使所有尚未撤銷的或有效期仍未屆滿的證書在該機關終止服務時得以撤銷，不論登記人是否有提出撤銷證書的要求；及

(e) 作出適當的安排，令認可核證機關儲存庫內的資訊（包括認可核證機關發出的證書的詳情及該機關的公開密碼匙），得以有秩序地轉移。該等資訊須轉移至一名保管人。由認可核證機關終止運作的日期或由資訊完成轉移的日期（以較遲的日期爲準）起計最少七年之內，該保管人須負責保管資訊。該等資訊的用途必須與認可核證機關的原來服務的用途一致，而接達該等資訊的方法及程序則須公布周知。

12 對遵守條例及本業務守則的評估

12.1 認可核證機關必須向總監提交報告如下：

(a) 最少每 12 個月提交一份報告，該報告須載有一份評估，說明該機關在報告所涵蓋的期間是否已遵守附錄 2 第 1 段所指明的條例及本業務守則的條文；

(b) 在該機關申請認可續期時提交報告，該報告須載有一份評估，說明該機關是否遵守以及有沒有能力遵守附錄 2 第 1 段所指明的條例及本業務守則的條文；及

(c) 在總監就該機關的重大變更而提出要求時，提交一份報告。該報告須載有一份說明以下事項的評估：

- 鑑於該機關已出現的重大變更，該機關是否遵守以及有沒有能力遵守附錄 2 第 3 段所指明的條例及本業務守則的條文；或

- 鑑於該機關將會出現的重大變更，該機關有沒有能力遵守附錄 2 第 3 段所指明的條例及本業務守則的條文。

12.2 認可核證機關須確保該報告是由一名獲總監爲此目的而認可爲合資格的人所擬備，擬備費用由該機關負擔。可獲考慮核准爲合資格擬備評估報告的人應具備下列條件：

- 獨立於接受評估的認可核證機關以外；
- 通過認可的專業團體或協會的評審；及
- 熟識下列工作範圍：
  - 對公開密碼匙基礎建設及有關科技的評估，例如數碼簽署及證書等；
  - 資訊保安工具及技術的應用；
  - 進行財務檢討；
  - 進行保安檢討；及
  - 進行第三方檢討。

12.3 合資格的人可以是具備以上所有條件的個人，或是合夥經營或機構，而該合夥經營或機構的成員整體上具備以上所有條件。簽署評估報告的個人必須：

- 是認可專業團體或協會的註冊會員，例如持有有效的執業證書或具備同等資格；
- 承擔整體責任，以確保進行評估程序的人在數碼簽署和證書、公開密碼匙基礎建設、財務事宜等各方面具備足夠的知識；及

- 承擔整體責任，以確保評估的質素及評估工作符合爲該等評估所訂下的標準或作業實務。

12.4 下列符合第 12.2 及 12.3 段所載要求的人士，可向總監申請獲核准爲有資格進行評估的人：

(a) 執業會計師（即持有根據《專業會計師條例》（第 50 章）發出的執業證書的會計師）；及

(b) 香港工程師學會資訊界別的法定會員，並同時爲根據《工程師註冊條例》（第 409 條）在同一界別下註冊的註冊專業工程師。

此外，總監亦可核准由其他人士提出的申請，認可他們爲有資格進行評估的人。

12.5 第 12.2 段所提述的專業團體或協會必須備有已確立的制度，以恰當地接納及規管其會員。該制度的主要特徵必須包括但不限於：

- 規範入會條件的規則和規例，例如培訓、能力測試、成爲會員的合宜程度等；

- 規範會員的專業及道德標準的規則和規例，以及規範會員專業服務表現的指引，例如處理利益衝突、執行和接受指示的表現；

- 推行會員的專業和道德標準及監察會員行爲操守的機制，包括但不限於正式的紀律處分程序、質量保證措施（例如同事之間的檢討）；及

- 強制性的接受持續專業進修的規定。

12.6 就第 12.1(a)分段所提述的評估報告而言，認可核證機關須在完成評估後的 4 個星期內向總監提交評估報告的文本。就第 12.1(b)分段所提述的評估報告而言，該機關須向總監提交在申請續期日期之前 4 個星期內完成的評估報告的文本。就第 12.1(c)分段所提述的評估報告而言，總監可於其就該機關的重大變更而發出的通知中，指明該機關須向總監呈交報告的時限。

12.7 認可核證機關向總監提交報告時，須同時向總監呈交關於其對合資格的人在評做報告中提出的例外情況、不足之處或建議的回應。

12.8 總監可能以認可核證機關未能符合條例、根據條例而訂立的規例以及業務守則內述明的規定爲理由，暫時吊銷或撤銷批給該機關的認可，或拒絕該機關提出將認可續期的申請。

13 聲明遵守條例及本業務守則的規定

13.1 認可核證機關必須向總監提交法定聲明如下：

(a) 最少每 12 個月提交一份法定聲明，述明該機關在法定聲明所涵蓋的期間是否已遵守附錄 2 第 2 段所指明的條例及本業務守則的條文；

(b) 在該機關申請認可續期時提交一份法定聲明，述明該機關是否遵守以及有沒有能力遵守附錄 2 第 2 段所指明的條例及本業務守則的條文；及

(c) 在總監就該機關的重大變更而提出要求時，提交一份述明以下事項的法定聲明：

- 鑑於該機關已出現的重大變更，該機關是否遵守以及有沒有能力遵守附錄 2 第 3 段所指明的條例及本業務守則的條文；或

- 鑑於該機關將會出現重大變更，該機關有沒有能力遵守附錄 2 第 3 段所指明的條例及本業務守則的條文。

13.2 認可核證機關須確保法定聲明是由該機關的負責人員作出，並由該機關負擔費用。

13.3 就第 13.1(a)分段所提述的法定聲明而言，認可核證機關須於作出法定聲明後的 4 個星期內向總監提交該份法定聲明。就第 13.1(b)分段所提述的法定聲明而言，該機關須向總監提交在申請續期日期之前 4 個星期內作出的法定聲明。就第 13.1(c)分段所提述的法定聲明而言，總監可於其就該機關的重大變更而發出的通知中，指明該機關須向總監呈交法定聲明的時限。

14 標準及技術的採用

14.1 認可核證機關須不斷檢討並在適當時改善和更新所採用的標準和技術，以保持登記人對該機關的信心及保障登記人的利益。該機關必須：

(a) 爲執行不斷檢討及在適當時更新標準和技術的職務而制訂明確的政策、管制措施和程序規則；

(b) 將上述職務指派予該機關內指定的組織；及

(c) 定期重新評估上述政策、管制措施和程序規則，以及有關組織的表現。

15 互通性

15.1 爲使認可證書所證明的數碼簽署在減少障礙的情況下取得廣泛接受，認可核證機關須盡可能採用開放及共通的界面，以協助其他人核實其認可證書所證明的數碼簽署。

15.2 認可核證機關須在核證作業準則內，述明其所支援的開放及共通的界面，以及與其他核證機關所建立的互通安排。

16 消費者的保障

16.1 認可核證機關就其服務所作的廣告，須內容得體、正確真實。在廣告內作出比較時亦須公平和不會產生誤導作用，而聲稱的所有事項均可逐一予以獨立地證實。

附錄 1 – 有關核證作業準則內容的標準及程序

1 引言

本附錄載列的標準及程序，是政府資訊科技總監（“總監”）根據《電子交易條例》（第 553 章）（“條例”）第 33 條發出的。該等標準及程序主要以互聯網工程專責小組（The Internet Engineering Task Force）的第2527號RFC文件《證書政策及核證作業架構》(RFC 2527 “Certificate Policy and Certification Practices Framework”) (一般稱爲《IETF PKIX第四部分》（IETF PKIX Part 4）)作爲基礎。所載列的標準及程序是總監預期認可核證機關在發出核證作業準則[1]時，須予採用及遵守的最低標準。

下文載列總監預期認可核證機關須符合的最低標準及最基本的程序。

2 主要特徵及核證作業準則簡介

2.1 主要特徵

認可核證機關須考慮就該機關發出的各類型、類別或種類證書的主要特徵作出概述。主要特徵會幫助登記人及倚據證書人士迅速了解根據核證作業準則發出的證書的有關特徵。

該等特徵須包括每類型、類別或種類證書的認可情況、證書的倚據限額及其他重要特徵，例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規定識別方式。此外，認可核證機關須提述由該機關用作提供其認可狀況及由總監備存的核證機關披露紀錄的網址或其他資訊來源。

2.2 核證作業準則簡介

2.2.1 概論

認可核證機關須就核證作業準則的目的及範圍提供高層次的摘要。該摘要應指明總監對該機關認可的範圍（例如認可的附帶條件），有關該認

[1] 核證作業準則的概念最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。核證作業準則不得與證書政策混淆，因爲兩者就作者、目的、具體程度及方法等方面均各有不同。

可對登記人及倚據人士的意義的概述及有關事宜。認可核證機關亦可強調核證服務的範圍、條款及條件。

2.2.2 識別

認可核證機關須就其核證作業準則提供適當的物件識別項目（如有的話）。如認可核證機關就其根據核證作業準則發出的認可證書而支援特定的證書政策，則該機關須識別該等政策，並須在核證作業準則的有關部分提供該證書政策的適當物件識別項目（如有的話）。此外，該機關須確保在可供登記人和準登記人以聯機方式接達的地點，公布所識別的政策的全文。

2.2.3 識別參與核證服務運作及維持核證服務的各方以及證書應用的範圍

認可核證機關須識別所有已知構成或參與認可核證機關運作及維持核證服務的團體或功能，例如核證機關功能、註冊功能、儲存庫及目標終端用戶（即登記人及倚據人士）。如有一項或以上的主要核證服務是以外發形式提供的（例如使用第三方註冊功能），須清楚述明。

此外，認可核證機關在適當的情況下，須載列該機關發出的每類型、類別或種類證書在應用方面的限制，例如：

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

2.2.4 聯絡資料

認可核證機關須最少提供一個聯絡點，以處理登記人及倚據人士作出有關規管及其他事宜的查詢。一般來說，認可核證機關最少會列出一個電話號碼、郵遞地址及電子郵址供登記人和倚據證書人士聯絡該機關。此外，認可核證機關須向登記人提供用作向該機關報告事件的熱線電話或其他途徑，以供登記人報告遺失密碼匙或密碼匙資料外洩等事件。

3 一般條文

3.1 責任

3.1.1 認可核證機關的職責和責任

認可核證機關須清楚述明該機關爲其提供的服務所承擔的職責和責任，包括條例載列的特定責任，連同作出認可的條件及本業務守則。該等責任的例子包括：

- 就發出證書一事向登記人（即該證書的發出對象）作出通知（包括作出該等通知的時間）；及
- 就撤銷或暫時吊銷證書一事向該證書的登記人作出通知（包括作出該等通知的時間）。

凡認可核證機關以外發形式執行其任何功能，與該等功能有關的職責和責任須另行闡述。

3.1.2 登記人的職責和責任

認可核證機關須闡述指配與該機關的登記人的職責及責任，包括在該機關支援的證書政策內載列的規定，例如：

- 確保在申請證書時所作的陳述準確無誤；
- 保障登記人的私人密碼匙；
- 對私人密碼匙及證書的使用施加限制；及
- 就私人密碼匙資料外洩或遺失作出通知。

3.1.3 倚據人士的責任

認可核證機關須按照核證作業準則的規定，清楚述明須向倚據人士作出的所有陳述，包括該機關所支援的任何證書政策，例如：

- 倚據人士須了解使用該證書的目的；

- 倚據人士須核實數碼簽署的責任；
- 查證撤銷及暫時吊銷證書的責任；及
- 確認接受適用的法律責任限制及保證。

3.1.4 儲存庫的責任

認可核證機關須清楚述明該機關就提供儲存庫服務所承擔的責任，包括條例載列的特定責任，其中包括核證機關的認可條件及本業務守則。該等責任的例子包括及時公布證書及撤銷證書（包括在適合的情況下暫時吊銷證書）的資訊，以及有關儲存庫可供接達和可供使用的條款。

3.2 法律責任

認可核證機關須清楚指明任何與攤分責任有關的適用條文，包括在登記人及本業務守則內界定的獲適當授權的人提出撤銷或暫時吊銷證書的要求之時起，至該機關實際撤銷或暫時吊銷證書之時止的一段期間內，利用證書作爲支援而進行的交易的處理方法。

此外，認可核證機關須清楚指明每項述明的倚據限額的影響。在任何情況下，本部分均不得被視爲豁免或彌償該機關，使其免負任何法律上不能豁免的法律責任。

3.2.1 保證及保證的限制

認可核證機關須就其發出的每類型、類別或種類的證書，清楚指明其有意採用的任何保證及／或施加的限制。

3.2.2 損害賠償的涵蓋範圍及卸責聲明

認可核證機關須就其發出的每類型、類別或種類的證書，清楚指明其法律責任的涵蓋範圍（例如直接的、間接的、特別的、相應的、突發的及算定損害賠償）以及任何卸責聲明和責任限制的範圍。

3.2.3 損失限制

認可核證機關須就其發出的每類型、類別或種類的證書，清楚指明每張證書或每宗交易的損失限制。

3.2.4 其他豁免事項

認可核證機關須就其發出的每類型、類別或種類的證書，清楚指明其他適用的豁免事項。

3.3 財務責任

認可核證機關須指明與該機關及其他任何在核證作業準則內識別的人士的財務責任的有關事宜，範圍包括：

- 受信關係會否在核證作業準則內識別的人士之間出現，或會否因發出證書而在有關人士之間出現；
- 行政程序的財政責任；
- 認可核證機關就其潛在或實際的法律責任以及針對其證書的倚據限額而提出的申索，向登記人及倚據人士提供的財務保證；及
- 其他財務方面的事宜，例如履約保證金、保險單，或其他由認可程序引致的責任（例如作爲認可條件之一的責任）。

3.4 釋義及執行

3.4.1 管限法律

認可核證機關須述明該機關及其核證作業準則，登記人協議及倚據人士協議的管限法律及司法管轄區。

3.4.2 解決爭議程序

認可核證機關須述明該機關所制訂的、用以解決有關其運作及因該機關向登記人或倚據人士所作陳述所引致的爭議及申索的程序。該等程序須

最少指出向該機關提出爭議或申索的程序，以及該機關對於在接獲申索或爭議的通知程序後所採取的步驟。

3.5 收費

認可核證機關須就其發出的每一類別、類型或種類證書的發出、撤銷、暫時吊銷、檢索或核實證書狀況，清楚述明向登記人及倚據人士收取的所有費用。

3.6 公布及儲存庫

認可核證機關須指明該機關所採用的政策及機制，以向其登記人及倚據人士提供有關其證書、其核證作業準則（包括該機關所支援的任何證書政策細節）、以及該機關的現行認可狀況及其發出證書的現行認可狀況等資訊。該機關應最少述明包括公布辦法、公布頻密程度、資訊是否可供取閱、接達儲存庫的管制措施及儲存庫的細節。

核證作業準則的全文，或一份刪去運作細節以免對認可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，須在該機關的網頁或其他可供方便接達的地點清楚展示出來。

由於認可核證機關所依循的實際程序預期會逐趨完善，核證作業準則的更新內容須在切實可行的範圍內盡快公布。所有變更須在展示核證作業準則的同一地點清楚展示出來，並在切實可行的範圍內盡快向總監報告。

3.7 關於遵守規定的評估

認可核證機關須述明有關該機關的遵守規定評估的機制及頻密程度，包括根據條例及本業務守則的任何強制性規定。具體範圍可包括：

- 就認可核證機關及其任何以外發形式執行功能進行遵守規定評估的頻密程度；
- 執行評估的獨立評估人的身分和資歷；
- 評估人與接受評估的認可核證機關之間的關係；
- 評估內容涵蓋範圍；及

- 有關傳達遵守規定評估的結果的政策（即報告文本的收件人）及跟進行動的政策。

3.8 保密政策

認可核證機關須指明該機關維持資訊保密的政策。須特別注意的事項包括：

- 認可核證機關（包括任何以外發形式執行的功能）須保持機密的資訊的類型；
- 不屬機密的資訊的類型；
- 有權獲告知證書被撤銷或暫時吊銷的原因的人；
- 發放資訊的政策，例如：提供資訊給執法人員，在法律程序下被要求披露等；
- 有關發放紀錄及資訊的政策；
- 認可核證機關（包括任何其以外發形式執行的功能）可因應資訊擁有人的要求／同意而披露資訊的情況；及
- 任何其他可以披露機密資訊的情況。

總括來說，認可核證機關須遵守有關個人資料的私穩的所有適用規例，而核證作業準則的條文則不得抵觸香港特別行政區現行有關私穩的規例及條例第 46 條的規定。

3.9 知識產權

認可核證機關須顧及關於證書、證書的撤銷／有效性的資訊、核證作業準則、證書政策、作業實務／政策的規定、名稱及密碼匙的知識產權。

4 識別及認證

認可核證機關須載列該機關或其外發的註冊機構功能（如適用的話）在發出證書前對證書申請人進行核實的程序。該機關發出的每一類別、類型或種類證書的程序均須予以闡述。

此外，認可核證機關須涵蓋證書密碼匙更新或在撤銷後證書密碼匙更新的核實程序。該機關亦須顧及與命名有關的作業實務，例如：名稱擁有權、名稱爭議及解決方法。

認可核證機關須指明其接受的各種識別方式，例如：香港身分證、護照、公司章程及商業登記證等。

4.1 初步核證

認可核證機關須指明在發出新證書時採取的身分證明和認證程序及命名方式。認可核證機關須涵蓋該機關用以證明證書申請人身分而所採取的特定程序，包括該機關在發出證書給證書申請人前該個人或團體須提交的特定文件。

4.1.1 名稱種類

認可核證機關須指明該機關所採用的命名常規，如“X.500 特定名稱”(X.500 Distinguished Names)或適用於網站證書的其他命名方式。其他的命名方式（例如電子郵址或個人識別號碼）也可包括在內，以確保個人的證書可清楚地加以識別。

認可核證機關亦須指明所有命名方式的細節，包括可能會採用的前綴及常規，以防止相同名稱的出現。

4.1.2 名稱是否應具意義

認可核證機關須指明證書內的名稱是否須具有意義（即使用獲廣泛理解的語義以描述個人或機構的身分）。如證書內的名稱應該具有意義，則應指明該機關所採取的程序，以確保所發給登記人的特定名稱具有意義並能適當地識別登記人。

4.1.3 闡釋不同命名形式的規則

認可核證機關須提供爲根據核證作業準則發出的證書所載的名稱格式而設的闡釋指引。這範圍的深入程度取決於證書所載的名稱格式。一般來說，如證書所載名稱的闡釋有可能爲倚據人士誤解，認可核證機關須考慮向倚據人士提供指引以減少產生錯誤闡釋的風險。

4.1.4 名稱的獨特性

如證書所載的名稱規定須具有獨特性，認可核證機關須制定規格以供依循。如證書的名稱須保存獨特性，認可核證機關須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特性。

4.1.5 解決命名爭議的程序

在適合的情況下，認可核證機關須指明該機關解決命名爭議的有關程序。

4.1.6 證明管有私人密碼匙的辦法

如證書申請人產生本身的配對密碼匙，而且只有其本人能控制該私人密碼匙，認可核證機關必須述明該機關如何核實申請人的私人密碼匙與申請人送交該機關以供核證的公開密碼匙是對應的。

4.1.7 登記人身分的核實

認可核證機關須指明該機關爲確保證書上的登記人與獲發證書的證書申請人的名稱相符而採取的程序。如認可核證機關採取特別的程序，以核實載於或將會載於證書上的申請人資訊（申請人名稱除外），該機關須列明該等特別程序。該等資訊將有助於使申請人了解根據核證作業準則取得數碼證書的所需規定，以及幫助倚據人士了解並推斷出根據核證作業準則發出的證書的可靠性。

4.2 例行密碼匙更新及證書續期

認可核證機關須闡述該機關爲進行例行密碼匙更新及爲證書續期而採取的程序；如用以證明登記人身分的程序與證書首次註冊及發出時所採取的程序不同，尤須作此闡述。該機關須在其核證作業準則內述明證書是否可不作密碼匙更新而續期。

4.3 撤銷證書後的密碼匙更新

認可核證機關須指明該機關在撤銷證書後再進行補發時，會否採用與首次發出證書時不同的程序。

4.4 撤銷證書的要求

認可核證機關須指明在認證及處理撤銷證書的要求時所採取的程序及機制，例如：

- 何人獲授權提出撤銷證書的要求，以及在何種情況下提出此要求；
- 撤銷證書的影響；
- 證書撤銷後，關於該證書的有效性的資料最快會在何時公布；
- 登記人對於引致證書須予撤銷的事件作出報告的責任；及
- 在有人提出撤銷證書的要求時對登記人所給予的保障，包括該核證機構與登記人的法律責任攤分的情況。

4.5 暫時吊銷證書的要求

認可核證機關須指明該機關是否支援暫時吊銷證書服務，如該機關提供這項服務，則須詳細列明暫時吊銷證書的條件及其影響。認可核證機關須具體指明暫時吊銷證書將如何執行，並且在適合的情況下，亦須包括第 4.4 段中就吊銷證書而提及的相同的事項。

5 操作方面的規定

5.1 申請證書

認可核證機關須說明與證書申請人申請新證書有關的詳情，包括：

- 申請證書的方法及規定提交用以證明申請人身分的文件；

- 有關的資訊，包括但不限於登記人的責任，認可核證機關的陳述、證書的條款及條件、核證機關及證書的認可狀況及認可狀況對登記人的意義（證書並非認可證書時尤須注意這點）；及

- 用以提交申請的界面規定。

5.2 發出證書

認可核證機關須說明該機關在發出證書時所依循的具體程序詳情。發出證書的程序包括：

- 密碼匙的產生；

- 把密碼匙交付適合人士（即是，如密碼匙由證書申請人所產生，該公開密碼匙必須與申請證書的要求一併交付認可核證機關，而該機關必須核實申請人管有對應的私人密碼匙。如密碼匙由認可核證機關所產生，私人密碼匙必須穩妥地交付申請人，而該機關必須列明所採取的適合措施，以確保其所管有的密碼匙得到適當的處理）；

- 在未取得登記人書面同意的情況下，認可核證機關不得管有登記人的私人密碼匙；

- 證書的產生；

- 把證書交付申請人；及

- 在儲存庫公布證書。

5.3 接受證書

認可核證機關須界定技術或程序方面的機制，以：

- 向證書申請人解釋第 3.1.2 段所界定的他們作爲登記人的責任；

- 通知申請人證書已經發出及證書所載的關於申請人的資訊；

- 容許申請人接受或拒絕接受該證書；及

- 協助申請人從核證機關取得證書。

認可核證機關須確保申請人在接受證書前有機會核實已經或將會載於證書的關於申請人的資訊。

5.4 暫時吊銷及撤銷證書

認可核證機關須解釋用以暫時吊銷或撤銷證書的程序。此外，該機關須說明登記人或獲適當授權人指示該機關暫時吊銷或撤銷證書的程序。

5.4.1 暫時吊銷證書

認可核證機關須提供暫時吊銷證書的詳細程序，包括：

- 暫時吊銷證書的條件（包括但不限於何人可以指令／撤回暫時吊銷證書）；
- 要求／指令暫時吊銷證書的方式；
- 暫時吊銷證書的公告方式（例如透過通告、電子郵件、把該證書納入證書撤銷清單內或任何其他公布有關暫時吊銷資訊的方式）；
- 撤回暫時吊銷證書或把暫時吊銷證書改爲撤銷證書的條件，例如時限；
- 認可核證機關暫時吊銷認可證書的所需時間，以及在登記人或獲適當授權人要求暫時吊銷證書與證書實際被暫時吊銷之間的一段期間內，因使用證書進行交易引致的法律責任的攤分；
- 認可核證機關向登記人或獲適當授權人查證該遭暫時吊銷的認可證書於暫時吊銷期過後應否予以撤銷或是恢復其有效性的預計時限；及
- 如認可核證機關不能接觸登記人或獲適當授權人以確定該遭暫時撤銷證書的最終安排時，該機關所採取的行動。

5.4.2 撤銷證書

認可核證機關須提供撤銷證書的詳細程序，包括：

- 撤銷證書的條件（包括但不限於何人可指令／撤回撤銷證書）；
- 要求／指令撤銷證書的方式；
- 作出撤銷的公告方式（例如透過通告、電子郵件、把該證書納入證書撤銷清單內、更新載有撤銷證書／證書有效性的資訊的伺服器或任何其他公布有關撤銷資訊的方式）；及
- 認可核證機關撤銷認可證書的所需時間，以及在登記人或獲適當授權人要求撤銷證書與證書實際被撤銷之間的一段期間內，因使用證書進行交易引致的法律責任的攤分。

登記人或獲適當授權人可使用能識別將被撤銷的證書、能解釋撤銷證書的理由及能核實撤銷證書要求（如數碼或人手簽署）的界面，提出撤銷登記人的證書的要求。撤銷證書要求的認證是十分重要的，因爲這措施可以防止未獲授權人惡意提出撤銷證書的要求。傳送要求的方式，例如電子郵件及網絡界面，須隨時可供登記人及獲適當授權人使用。

一般來說，證書在下列情況下須予以撤銷：

- 證書內的識別資訊或特徵在證書有效期屆滿前有所變更；
- 知悉登記人已違反對應的核證作業準則的規定；
- 登記人懷疑或確認私人密碼匙的資料外洩；或
- 登記人不再希望擁有或需要簽署電子訊息的能力。

5.4.3 證書撤銷清單及其他公布有關撤銷資訊的方式

證書撤銷清單指明由認可核證機關發出但已經被撤銷的證書，並可就每一證書說明其撤銷理由。認可核證機關須述明分發證書撤銷清單的機制，及倚據人士如何接達該等清單，並須指明更新證書撤銷清單的頻密程度。

認可核證機關可決定使用或支援任何其他公布有關證書撤銷資訊的方式。認可核證機關須說明可供使用的接達資訊機制、有關機制的使用條款和條件及有關資訊的更新頻密程度。

5.4.4 就證書撤銷清單或其他公布有關撤銷資訊的方式而規定的查核要求

認可核證機關須通知登記人及在一般可以接達的地點明顯地作出通告，指出如載有公開密碼匙以核實數碼簽署的證書不再有效，倚據該數碼簽署是具有風險的。

此外，認可核證機關須清楚地及明顯地指明其在倚據人士暫時不能取得有關撤銷證書的資訊（而如該認可核證機關亦透過證書撤銷清單或其他公布有關撤銷資訊的方式公布有關證書暫時吊銷的資訊，則亦包括有關證書暫時吊銷的資訊）的情況下所採取的政策。認可核證機關須特別指出在這種情況下的攤分法律責任的問題。

5.5 保安覆檢程序

認可核證機關須闡述該機關所採用的事件記錄及覆檢系統，以維持一個安全的運作環境。該等系統包括的範圍如下：

5.5.1 所記錄事件的類型

認可核證機關須闡述該機關將會記錄的事件的類型。認可核證機關最少須考慮記錄下列事件：

- 電腦設施的行政管理，包括但不限於：
  - 網絡上的可疑活動；
  - 重覆的未能接達的情況；
  - 與就核證機關的整體運作而設置的設備和軟件的安裝、修改及組態設定有關的事件；
  - 使用特許方式接達核證機關各部分的事件；及

- 一般的證書管理運作，例如：
  - 撤銷及暫時吊銷證書的要求；
  - 實際發出（包括向認可核證機關申請認可證書的任何人的身分證明文件）、撤銷及暫時吊銷證書；
  - 證書續期；
  - 更新儲存庫；
  - 有關證書撤銷及暫時吊銷的資訊的產生及公布；
  - 核證機關密碼匙的產生以及密碼延續（包括有關文件）；
  - 登記人配對密碼匙的產生（包括有關文件）；
  - 備份；及
  - 緊急的密碼匙運作復原。

在切實可行的範圍內，所記錄的事件須識別引發該事件的單位或個人，以及包括任何作出回應的行動及採取行動的人員。所有紀錄內容須蓋上日期及時間。

認可核證機關首先根據現行獲接納的作業實務，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限，是良好的作業方法。所有超出界限的事件和重要趨勢必須加以記錄。

認可核證機關須區分特權及實施其他機制或程序，以確保所有紀錄完整無誤。認可核證機關須闡述用以區分特權的機制及程序。

5.5.2 處理事件紀錄的頻密程度

認可核證機關須指明處理事件紀錄（例如綜合審核及檢討）的頻密程度。

5.5.3 事件紀錄的保存期限

認可核證機關須指明事件紀錄的保存期限，而該期限須符合本業務守則的規定。

5.5.4 事件紀錄的保護

認可核證機關須指明爲保護事件紀錄免受意外損毀或蓄意修改而採取的機制。

5.5.5 事件紀錄備份的程序

認可核證機關須指明把事件紀錄備份的程序及備份的保留期限。良好的作業實務是要確保儲存設施能爲備份提供足夠的保護，以免備份遭盜竊和損毀或出現媒體衰變。此外，必須確保在存檔期間，數據的儲存和檢索方法是現行及有效的方法。

5.6 紀錄存檔

認可核證機關須闡述關於該機關保留一般紀錄的政策。一般來說，認可核證機關須確保其所存檔的紀錄的詳盡程度，足以確立在以往發出的證書的有效性及該機關在以往能妥善運作。認可核證機關可考慮存檔的主要數據類型包括：

- 與設立核證機關的設備有關的數據，如：
  - 系統設備的組態設定檔案；
  - 設備評估及／或設備評審檢討的結果（如曾經進行）；
  - 核證作業準則；及
  - 認可核證機關須予遵守的任何具合約性質的協議。
- 與認可核證機關的運作有關的數據：
  - 任何上述數據項目的修改或更新；

- 所有已發出的證書及已公布的有關證書撤銷及暫時吊銷的資訊；
- 定期的事件紀錄（根據第 5.5 段的規定）；及
- 其他用以核實存檔內容的所需資料。

5.6.1 存檔的保留期限

認可核證機關須指明存檔紀錄的保留期限，而該期限須符合本業務守則的規定。

5.6.2 存檔的保護

認可核證機關須指明用以保護存檔紀錄的程序，例如：

- 該等存檔的保管人；
- 接達該等紀錄的機制，例如：爲覆檢或解決爭議等目的；及
- 保護存檔免受意外損毀或蓄意修改、盜竊或媒體衰變的機制。

5.6.3 存檔備份的程序

認可核證機關須指明爲存檔紀錄備份的程序及備份的保留期限。良好的作業實務是要確保儲存設施能爲備份提供足夠的保護，以免備份遭盜竊和損毀或出現媒體衰變。此外，必須確保在存檔期間，儲存及檢索數據的方法是現行及有效的方法。

5.7 密碼匙變更

認可核證機關須指明該機關變更其密碼匙的程序及把有關程序通知登記人的機制。

5.8 密碼匙資料外洩及運作復原

認可核證機關須闡述該機關在密碼匙資料外洩或發生災難時發出通知及運作復原的程序。該機關須特別說明下列事項：

- 認可核證機關在其電腦資源、軟件及／或數據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運作復原程序。該等程序闡述如何重新建立穩妥可靠的環境、須予撤銷的證書、認可核證機關本身的密碼匙應否予以撤銷、如何爲登記人提供新的核證機關公開密碼匙及如何重新核證登記人的方法；

- 認可核證機關在密碼匙資料外洩或懷疑外洩時所採取的運作復原程序，包括通知登記人和倚據人士，及重建核證機關穩當運作的程序；及

- 在發生自然或其他災害後但在穩妥可靠的環境尚未在原地點或後備地點重新確立前，認可核證機關爲其設備作穩妥安排的程序，例如在受損毀的地點保護敏感資料免遭盜竊的程序。

如發生任何上述事件必須立即通知總監。

5.9 核證機關終止服務

認可核證機關須指明該機關終止服務及通知登記人及倚據人士有關其終止服務的安排，包括該機關的存檔紀錄保管人的身分。該等安排須遵守本業務守則第 11 段載列的規定。

6 實體、程序及人事保安方面的管制措施

認可核證機關須闡述該機關制定的非技術性運作管制措施，以保證其業務以穩當的方式進行。

該等管制措施的主要例子包括核證機關主要功能的實體、程序及人事方面的管制措施；核證機關的主要功能計有密碼匙的產生、證書申請人身分的核實、證書的發出、證書的撤銷或暫時吊銷、審核、存檔等。核證機關亦可就儲存庫及任何以外發形式執行的功能（例如註冊功能）制訂類似的管制措施。

6.1 實體保安管制措施

認可核證機關須闡述對裝載該機關系統的設施的管制措施，其中包括：

- 場地的地點及結構；
- 識別保安範圍及實體進入有關範圍的考慮因素；
- 環境災患，例如：電力供應、空氣調節、濕度、水災、火災等；及
- 媒體儲存及處置。

6.2 程序管制措施

就認可核證機關的運作而言，獲信任職位指某些職位，其擔任人士無論是因意外或蓄意而引致不恰當地執行其職責，便可能令該機關出現保安問題。獲信任職位包括負責監管的管理人員及操作人員。獲得選擇擔當該等職位的人必須具備所需才能及足以勝任。該等職位所發揮的功能是整個核證機關進行穩當運作的基礎。

認可核證機關須闡述該機關識別人選擔任獲信任職位（例如產生認可核證機關密碼匙）的程序，及界定該等職位的責任。一般來說，該等程序的規定會指明將執行的工作、執行每項工作的所需人數及職級，及將會推行的管制措施如雙重管制、識別以至認證有關人士等。

獲信任職位的例子包括：

- 核證機關行政主管——負責監察所有證書的發出、認可核證機關的運作及收集及備存紀錄。基本來說，核證機關行政主管應確保該機關的核證機關功能按照其核證作業準則內的規定執行；
- 密碼匙復原代理人——與備存密碼匙復原資料或系統有關的特定功能的負責人員；及
- 其他獲信任職位——認可核證機關可在核證機關行政主管的監督下界定其他角色。該等角色須按照核證作業準則內的有關條文執行特定功能。在適當的情況下，所有對系統完整性有潛在影響的運作須實行區分職責的措施。

6.3 人事保安管制措施

認可核證機關須闡述有關該機關人員的聘用、監察、評估、培訓及終止僱用的管制措施。可予說明的具體事項包括：

- 聘用程序，包括對招聘擔任獲信任職位及其他執行敏感程度較低的職位的人士進行的背景審查和保安查核程序；
- 培訓規定及程序，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頻密程度及次序；
- 工作表現評核架構，及對擅自行動、不適當使用權力及擅自使用認可核證機關系統的人員採取的紀律處分和終止僱用的程序；
- 對合約人員的管制措施，包括合約內的規定，例如：合約人員須就其行動所引致的損失作出彌償，以及監察合約人員的工作表現等；及
- 爲有關人員提供的文件，例如：使用者手冊、操作程序等，以支援該等人員執行職務。

7 技術保安管制措施

認可核證機關須界定該機關制訂的技術保安措施，該等措施特別用於保護其密碼匙及啓動數據（例如：個人識別密碼、密碼等）。此外，該機關可闡述其打算對儲存庫或登記人等採取的任何規定或限制，以確保其密碼匙及關鍵的保安參數得到適當的保護。穩妥的密碼匙管理對維持穩當系統甚爲重要。它確保所有私人密碼匙及啓動數據受到保護，並且只有獲授權人才可使用。此外，認可核證機關須闡述該機關所採用的其他技術保安管制措施，以支援密碼匙及證書管理的運作。

認可核證機關所執行的管制措施必須與其他人士的管制措施，例如任何以外發形式執行的功能（如註冊功能、儲存庫等）以及登記人所執行的管制措施分開，以清楚識別有關方面的責任。

可予說明的具體管制範圍包括：

- 配對密碼匙的產生、安裝，及配對密碼匙管理工作的其他方面，包括：
  - 產生公開及私人配對密碼匙的責任；
  - 把私人密碼匙穩妥地交付證書申請人（如該配對密碼匙是由認可核證機關爲申請人而產生的）；
  - 把申請人的公開密碼匙穩妥地交付發出證書的人（如該配對密碼匙是由申請人產生的）；
  - 把認可核證機關的公開密碼匙穩妥地交付登記人；
  - 所採用的密碼匙大小（可供使用的技術須予以考慮）；
  - 有關公開密碼匙參數的產生及品質檢查的管制措施；
  - 所使用的密碼模組類型及品質的規定；及
  - 密碼匙的使用及目的 (根據《X.509 公開密碼匙基礎建設證書結構》（第三版）及《證書撤銷清單結構》（第二版）(X.509 PKI Certificate Profile version 3 and CRL Profile version 2)的標準在密碼匙使用旗標上作出標示)。
- 私人密碼匙的保護，例如：
  - 密碼匙產生模組的規定標準(如有的話)，例如符合《ISO 15782-1/ FIPS 140-1 密碼模組的保安規定》（ISO 15782-1/ FIPS 140-1 Security Requirements for Cryptographic Modules）的某個水平的標準；
  - 對私人密碼匙使用多人管制的措施；
  - 把私人密碼匙備份，包括備份的形式及備份系統的有關保安管制措施；

- 私人密碼匙存檔，包括存檔密碼匙的形式及存檔系統的有關保安管制措施；

- 對私人密碼匙啓動、使用及停止啓動的管制措施，包括密碼匙數據輸入所需的人數、私人密碼匙的形式、啓動機制、已啓動的密碼匙的生效期等；

- 有關銷毀密碼匙的管制措施，例如：交出權標、銷毀權標或重寫密碼匙；

- 公開密碼匙存檔；及

- 公開及私人密碼匙的使用期間。

- 啓動數據的管制措施，扼要列出啓動數據生命周期(即由產生、分派至存檔及銷毀的過程)的管制措施。管制措施的考慮因素應與上文闡述的產生配對密碼匙及保護私人密碼匙的考慮因素相似；

- 電腦保安管制措施，扼要列出爲防止及偵測認可核證機關系統的擅自接達、修改或資料洩漏所採取的保安措施。適當的電腦保安級別架構可予參考，例如《ISO 15408：1999 資訊科技保安評估通則》(ISO 15408：1999 Common Criteria for Information Technology Security Evaluation (CC))；

- 系統發展生命周期管制措施，扼要列出認可核證機關對系統發展生命周期所採取的管制措施，涵蓋爲初次配置的認可核證機關設備而採購或發展的軟件及硬件的機制和程序，以防止擅自改動的情況；

- 網絡保安管制措施，扼要列出保護認可核證機關設備所有連接情況的管制措施，例如：適當配置及維持的防火牆，或相等的接達管制裝置，及監察嘗試擅自接達的情況並防止遭受惡意的攻擊；及

- 密碼模組工程管制措施，扼要列出密碼模組的具體管制規定。在制訂管制措施時，可參考適合的標準，例如《ISO 15782-1/FIPS 140-1 密碼模組的保安規定》(ISO 15782-1/FIPS 140-1 Security Requirements for Cryptographic Modules)。

8 證書及證書撤銷清單的結構

認可核證機關須指明核證機關採用的證書格式、證書撤銷清單的格式及公布證書撤銷資訊的任何其他方式的格式（如適用），包括結構、版本及所使用的伸延的資訊。認可核證機關一般會根據《ITU X.509》(第三版)（ITU X.509 v3）的證書格式發出及管理公開密碼匙證書，並根據《ITU X.509》(第二版)（ITU X.509 v2）的證書撤銷清單格式產生及公布證書撤銷清單。

認可核證機關須盡可能採用獲廣泛接受的標準，以促進使用證書的應用系統之間的互通性。因此，在證書及證書撤銷清單方面，極力建議使用符合《RFC 3280 互聯網 X.509 公開密碼匙基礎建設證書及證書撤銷清單結構》(RFC 3280 Internet X.509 PKI Certificate and CRL Profiles)（或互聯網工程專責小組其後公布的任何更新版本）的標準，及避免使用關鍵的伸延。

8.1 證書結構

認可核證機關須提供與證書結構的具體規格有關的資訊，涵蓋範圍可載列如下：

- 所支援的版本編號；
- 證書所使用的伸延，特別是已有內容的伸延及其關鍵性；
- 加密算法的物件識別項目;
- 所使用的名稱形式；
- 命名限制；
- 證書政策的物件識別項目；
- 政策限制伸延的使用；
- 政策識別字段的語法及語義；及
- 主要的證書政策伸延的語義處理。

8.2 證書撤銷清單的結構

認可核證機關須提供與證書撤銷清單有關的資訊，並可提述適合的標準，涵蓋範圍包括：

- 證書撤銷清單所支援的版本編號；及
- 證書撤銷清單所採用的資料伸延及其關鍵性的詳情。

如認可核證機關採用其他方式公布有關證書撤銷的資訊，該機關須提供關於該公布方式的資訊，以便其他人士得以接達有關證書撤銷的資訊。

9 規格的管理

認可核證機關須闡述如何備存核證作業準則。

9.1 規格的變更程序

認可核證機關須闡述對核證作業準則作出任何變更的程序，包括根據本業務守則載列的規定把有關的變更通知總監、登記人及倚據人士的機制。認可核證機關須盡快在該機關的儲存庫內公布及提醒對核證作業準則作出的變更。此外，該機關可指明無須給予事先通知的變更的類型。

9.2 公布及通知程序

認可核證機關須闡述在所有登記人及倚據人士知悉的儲存庫公布所有有關資訊的程序，而該儲存庫可以是一個網站。認可核證機關必須指出該儲存庫的位置及其他的資訊來源。

10 互通性

爲促進互通性，認可核證機關須採用獲廣泛接受的技術標準及管理措施。爲方便應用系統使用其證書及服務，認可核證機關須在適當的情況下指明其所採用的標準及作業實務，以及已選定的選項及界面規格的詳情。認可核證機關須公布的詳情包括但不限於其儲存庫採用的標準（例如：對目錄的輕量式目錄接達規約（LADP）或兼容規約、網頁的超文本標示語言（HTML）等)，及具體的證書結構（例如 X.509）、證書伸延等。

附錄 2 — 就核證機關的評估而指明的《電子交易條例》及本業務守則的條文

1 爲施行《電子交易條例》（第 553 章）（“條例”）第 20(3)(b)(i)、27(5A)(b)(i)及 43(1)(a)(i)條而指明的條例及本業務守則的條文

1.1 條例的下列條文屬於獲總監認可爲合資格人士所作評估的範圍：

(a) 第 VII 部 — 總監對核證機關及證書的認可：
第 21(4)(a)、(b)、(c)及(f)條。

(b) 第 X 部 — 關於認可核證機關的一般條文：
第 36、37、39、40、42(1)及(2)、44 及 45(1)條。

(c) 第 XI 部 — 關於保密、披露及罪行的條文：
第 46、47 及 48 條。

1.2 本業務守則的下列條文屬於獲總監認可爲合資格人士所作評估的範圍：

(a) 認可核證機關的一般責任：
第 3.1 至 3.6 各段及第 3.8 段。

(b) 核證作業準則：
第 4.1 至 4.13 各段。

(c) 穩當系統：
第 5.1 至 5.3 各段、5.6 至 5.17 各段及 5.19 至 5.21 各段。

(d) 證書及認可證書：
第 6.1 至 6.23 各段。

(e) 登記人身分的核實：
第 7.1 及 7.2 段。

(f) 倚據限額以及爲法律責任投保：
第 8.1 至 8.4 各段。

(g) 儲存庫：
第 9.1 至 9.5 各段。

(h) 披露資訊：
第 10.1 至 10.6 各段。

(i) 終止服務：
第 11.1 至 11.5 各段。

(j) 對遵守條例及本業務守則的評估：
第 12.1 段。

(k) 聲明遵守條例及本業務守則的規定：
第 13.1 段。

(l) 標準及技術的採用：
第 14.1 段。

(m) 互通性：
第 15.1 及 15.2 段。

(n) 附錄 1：
本業務守則附錄 1 所有段落。

2 爲施行條例第 20(3)(c)(i)、27(5A)(c)(i)及 43(1)(b)(i)條而指明的條例及本業務守則的條文

2.1 條例的下列條文須以核證機關一名負責人員作出法定聲明的方式處理：

(a) 第 VII 部 — 總監對核證機關及證書的認可：
第 21(4)(e)條。

2.2 本業務守則的下列條文須以核證機關一名負責人員作出法定聲明的方式處理：

(a) 認可核證機關的一般責任：
第 3.7 及 3.9 段。

(b) 穩當系統：
第 5.18 段。

(c) 披露資訊：
第 10.7 至 10.9 各段。

(d) 消費者的保障：
第 16.1 段。

3 爲施行條例第 43A(1)(c)(i)及(d)(i)條而指明的條例及本業務守則的條文

3.1 視乎認可核證機關將會或已經對其系統、運作、管制措施及程序作出的重大變更的具體情況而定，總監會在他根據條例第43A(1)條可向認可核證機關發出的通知中，爲施行條例第43A(1)(c)(i)及(d)(i)條而指明條例及本業務守則的相關條文。