認可核證機關業務守則擬稿的公眾諮詢

政府致力推動電子貿易在香港發展。為確保電子交易可在穩妥可靠的情況下進行，政府將為核證機關的運作設立一套機制。政府不會向在香港經營的核證機關實施強制性的發牌制度，但為了保障消費者的權益，政府建議設立一套自願申請認可的制度。有關建議的內容已在交予立法會審議的《電子交易條例草案》中詳細說明。草案建議由資訊科技署署長(下文簡稱「署長」)向核證機關發出認可。

2. 向署長申請認可的核證機關在運作上必須達至政府認為穩妥可靠的水平，並且應當採用開放共通的界面，確保可與其他認可核證機關互相配合運作。在自願申請制度下獲得認可的核證機關必須遵守署長所發出的業務守則。守則載列核證機關的一般責任及其運作上所需遵照的標準及程序。認可核證機關如未能符合該守則的規定，署長發出的認可可被暫時吊銷或撤銷。

3. 政府現在公布認可核證機關業務守則的擬稿作公眾諮詢，歡迎各界就擬稿發表意見。請於一九九九年十一月十五日或之前，採用下列任何一種方式把意見書送交資訊科技署:

郵寄	香港灣仔港灣道 12 號 灣仔政府大樓 15 樓 資訊科技署
傳真	2802 4549
電子郵址	enquiry@itsd.gcn.gov.hk

4. 對於各界就業務守則擬稿所遞交的意見書，政府保留公開全部或部分資料的權利。任何屬於商業機密的資料，必須清楚註明，以便政府決定是否公布有關資料。

資訊科技署

一九九九年十月二十五日

認可核證機關

業務守則

(擬稿)

一九九九年十月二十五日

香港特別行政區政府

目錄

1. 引言 1

2. 用語定義 2

3. 認可核證機關的責任 8

4 儲存庫 23

5. 修訂業務守則 25

1. 引言

1.1 《電子交易條例》（下文簡稱「條例」）第 39 條訂明，資訊科技署署長（下文簡稱「署長」）可發出業務守則，指明認可核證機關在執行其功能時所需遵守的標準及程序。

1.2 本業務守則是署長根據條例第 39 條發出，指明認可核證機關在執行其功能時所需遵守的標準及程序。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，須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，須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），可考慮該認可核證機關未能遵守本業務守則的情況。

2. 用語定義

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 — – 由核證機關為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

核證機關披露紀錄　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

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

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　就核證機關而言，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、舞弊或不誠實的作為的裁斷；

– 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，亦沒有在核證機關申請成為認可核證機關的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，亦沒有在該核證機關申請成為認可核證機關的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。

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
認可核證機關	指署長根據條例第 20 條所認可的核證機關，或條例第 28 條所提述的核證機關
認可證書	指署長根據條例第 21 條所認可的證書，或屬署長根據條例第 21 條所認可的類型、類別或種類的證書，或條例第 28 條所提述的認可核證機關所發出的證書；並須由該認可核證機關指定為認可證書
負責人員	就核證機關而言，指在該機關與本條例有關的活動方面身居要職的人

認可儲存庫	指署長根據條例第 40 條所認可的儲存庫
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為獲發給證書； – 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

穩當方式	就記錄，備存及存檔資訊及紀錄而言，指能夠確保資訊及紀錄準確、安全、得以保密、完整及可供查閱以作檢索及檢查的程序及安排，而該等程序及安排與記錄，備存或存檔有關資訊及紀錄的原本目的相符
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，以確保只可由獲授權人士用已批准的方式查閱資料； – 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； – 以一致及準確的方式備存系統的數據和紀錄； – 合理地適合執行其原定功能；及 – 依循獲廣泛接受的安全準則。

3. 認可核證機關的責任

3.1 一般責任

3.1.1 認可核證機關必須遵守一切認可條件，包括署長根據條例第20條作出認可時所附加的條件。

3.1.2 認可核證機關必須遵守香港特別行政區的現行法律。

3.1.3 認可核證機關的行事方式，不得對其登記人或可能倚據其所發出的認可證書的人構成不合理的風險。

3.1.4 除本業務守則另有規定外，凡根據本業務守則認可核證機關須記錄，備存或存檔資訊及紀錄，該核證機關必須記錄，備存或存檔有關資訊及紀錄，為期不少於七年。

3.2 核證作業準則

3.2.1 認可核證機關必須就其所發出的每種類型、類別或種類的認可證書，向公眾公布及備存最新的核證作業準則。認可核證機關在公布核證作業準則時，須把該作業準則的副本呈交署長，而日後如對作業準則作出任何變更，亦須在切實可行的時間內盡快通知署長。

3.2.2 認可核證機關須就核證作業準則的每個版本以穩當方式保存一份副本，並記錄作業準則的生效日期和停止有效

日期。認可核證機關亦須記錄對作業準則所作出的一切變更，以及每項變更的生效日期。

3.2.3 認可核證機關在發出某類型、類別或種類的認可證書時，須遵守就該類型、類別或種類的證書所公布的核證作業準則。

3.2.4 認可核證機關須在核證作業準則內向登記人申明限制其法律責任的事項，尤其須促使登記人注意其認可證書所載列的倚據限額的含意。

3.2.5 核證作業準則須訂明為發出及續發某類型、類別或種類的認可證書而採取的核實登記人身分的程序。

3.3 穩當可靠

3.3.1 認可核證機關必須使用穩當系統以提供服務，包括發出、續發、暫時吊銷或撤銷認可證書；就認可證書的發出、續發、暫時吊銷或撤銷發出通知；或在認可儲存庫內公布認可證書。

3.3.2 認可核證機關須以穩當方式就以下事項作出及備存紀錄—

a. 發出、續發、暫時吊銷及撤銷認可證書的工作（包

括任何向認可核證機關申請認可證書的人的身分證明文件）；

b. 產生認可核證機關本身及登記人的配對密碼匙的有關文件；及

c. 認可核證機關電腦設施的管理。

認可核證機關須把其發出的一切認可證書存檔，並須維持查閱該等證書的機制。認可核證機關須以穩當方式保留本段指明須予保存的一切紀錄及就證書存檔所作的一切紀錄，以確保若要將有關紀錄複製給予署長或審核該認可核證機關的運作的人時，有關紀錄仍然準確、完整、可閱和可供查閱。

3.3.3 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的影響，該認可核證機關必須採取以下行動：

a. 盡合理程度的努力通知任何已知或可預見會受該事故影響的人士；

b. 如核證作業準則已訂明處理該類事故的程序，須按照該等程序行事；及

c. 就有關事故立刻通知署長。

3.3.4 認可核證機關須設置穩當系統，以產生其本身及登記人的配對密碼匙。

3.3.5 認可核證機關須以穩當方式，分開保存其本身的私人密碼匙及啟動數據（例如個人辨認號碼、密碼等）。

3.3.6 認可核證機關須確保所有負責人員和那些直接負責認可核證機關日常運作、保安及執行工作的人員，以及那些在職務上直接關乎發出、續發、暫時吊銷或撤銷認可證書（包括確認任何向認可核證機關申請認可證書的人士的身分）、產生私人密碼匙或管理認可核證機關電腦設施的人員 —

a. 均為適當人選；及

b. 具有可有效執行職務的相關知識、技術資格和專業知識。

3.4 證書

3.4.1 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。

3.4.2 認可核證機關須就所發出的每一類型、類別或種類的認

可證書，制定獨立的核證作業準則。

3.4.3 對於認可核證機關所發出但未經署長認可的證書，該認可核證機關須促使登記人及倚據其所發出證書的人士，注意有關使用及倚據該等證書的後果。

3.5 倚據限額

3.5.1 認可核證機關向登記人發出認可證書時，可根據條例內的條文在認可證書內訂明倚據限額。

3.5.2 認可核證機關必須在每一類型，類別或種類的認可證書的核證作業準則內，說明倚據限額對其所發出的該類型，類別或種類的認可證書有何含意。

3.5.3 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。

3.6 核實身分

3.6.1 認可核證機關必須在與每一類型，類別或種類的認可證書相關的核證作業準則內，說明以何種程序核實向認可核證機關申請該類型，類別或種類的認可證書的人士的

身分。有關程序必須指明該核證機關就該類型，類別或種類的認可證書核實申請人士身分的步驟，而該等步驟須與有關目的相符及遵從有關法例及規例。

3.6.2 認可核證機關必須把證明申請人身分的文件存檔。

3.7 披露資料

3.7.1 認可核證機關必須在其維持的認可儲存庫內公布：

a. 其載有公開密碼匙的證書，而有關的公開密碼匙與該認可核證機關用以為另一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批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。

3.7.2 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。

3.7.3 認可核證機關必須根據署長的指示，每隔一段時間呈交載有以下資料的進展報告：

a. 各類型，類別及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各類型、類別及種類證書的數目；

c. 相對於既定服務水平的表現；

d. 新發出的類型、類別及種類的證書；

e. 組織結構的改變；及

f. 自上次呈交進展報告或申請認可以來，以上各項資料的改變。

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。

3.7.4 如有任何特別事故影響認可核證機關的穩當可靠性，有關的認可核證機關必須立即向署長呈交報告。

3.7.5 認可核證機關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。

3.8 發出證書

3.8.1 認可核證機關必須在以下情況才可向申請人發出認可證書：

a. 收到申請人提交發出認可證書的要求；及

b. 遵照該類型，類別或種類認可證書的核證作業準則所載列的一切做法及程序，包括就申請該類型、類別或種類認可證書的人而核實其身分的程序。

3.8.2 認可核證機關必須維持載有所發出認可證書的儲存庫，並須在所維持的認可儲存庫公布其發出而又獲登記人接受的認可證書。

3.8.3 認可證書必須載有或以提述方式收納足以找到或確定一個或多於一個認可儲存庫的資料。如果有關認可證書被暫時吊銷或撤銷時，該等儲存庫必須載列有關的通知。

3.8.4 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。

3.8.5 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，將其所知並嚴重影響認可證書有效性或可靠性的任何事實告知登記人。

3.8.6 認可證書必須註明有效期在何日屆滿。

3.8.7 凡與發出認可證書有關的事項，包括日期和時間，均須以穩當方式記錄及保存。

3.8.8 認可核證機關發出認可證書，就相當於向合理地倚據認可證書或以認可證書所列載公開密碼匙核實的數碼簽署的人士表明，認可核證機關是按照以提述方式收納於認可證書內的任何適用的核證作業準則，或按照倚據認可證書或數碼簽署的人士已獲通知的核證作業準則，發出認可證書。

3.9 暫時吊銷及撤銷證書

3.9.1 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。

3.9.2 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. 認可證書內所指名的登記人；或

b. 獲授權代表該登記人行事的人士。

3.9.3 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，在有關證書內所指明的認可儲存庫內，公布經簽署的暫時吊銷或撤銷認可證書的通知。

3.9.4 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的可靠性，及決定是否恢復該證書的有效性或撤銷該證書。

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

3.9.6 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抑或恢復有關證書的有效性。

3.9.7 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，均須以穩當方式記錄及保存。

3.9.8 核證機關凡暫時吊銷（如可以將認可證書暫時吊銷）或撤銷所發出的認可證書，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。

3.10 認可證書的續期

3.10.1 認可證書可在有效期屆滿時續期。

3.10.2 凡與認可證書續期有關的事項，包括日期和時間，均須以穩當方式記錄及保存。

3.11 互通性

3.11.1 認可核證機關必須盡可能採用開放及共通界面，以便他人核實其發出認可證書所證明的數碼簽署。

3.12 標準及科技的應用

3.12.1 認可核證機關必須不斷檢討及更新所採用的標準和科

技，確保所採用系統及程序的穩當性，以保障登記人的利益。

3.12.2 建立數碼簽署所採用的技術必須確保：

a. 數碼簽署必須在與其相關的人士的指示下才能建立；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，任何人均不能複製數碼簽署及從而建立有效的數碼簽署。

3.13 審核

3.13.1 認可核證機關的運作必須根據條例的條文及本業務守則進行審核。審核亦須包括評估在發出認可證書時，該核證機關有否遵守其就該認可證書公布的核證作業準則。

3.13.2 所有審核工作均須由一位經署長核准的合資格及獨立的審計人員執行。

3.13.3 認可核證機關必須在每次審核工作完成後的四個星期內，向署長呈交有關的審核報告。若認可核證機關向署長申請續發認可資格，則必須呈交一份在申請日期

前三個月內完成的審核工作的報告。

3.13.4 署長可根據認可核證機關未能通過審核為理由，撤銷其獲批予的認可資格，或拒絕有關核證機關提出續發認可資格的申請。

3.13.5 認可核證機關須在其機構內設立內部審核單位，確保其運作符合條例的條文、本業務守則及核證機關就其認可證書公布的核證作業準則。

3.14 終止計劃

3.14.1 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。

3.14.2 終止服務計劃須指明核證機關終止服務時的安排，尤其是存檔其紀錄包括其所發出的證書為期不少於七年及確保登記人的利益得到適當照顧的安排。

3.14.3 認可核證機關如擬終止其服務，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，至少連續三日在一份英文日報及一份中文日報刊登有關擬終止服務的啟事；及

d. 如果署長認為有需要，該核證機關在終止其核證服務時作出安排，撤銷所有尚未撤銷或有效期仍未屆滿的證書。

3.15 保安及風險管理

3.15.1 認可核證機關必須採用獲普遍接受的保安準則及標準以制定保安政策，而保安政策涵蓋範圍至少必須包括核證機關運作方面的實質管制、程序管制、人事管制、技術保安管制及保安審核程序。

3.15.2 認可核證機關必須訂定全面的保安事故報告和處理程序及運作復原體系和程序。

3.15.3 認可核證機關必須充分地確定及制訂程序，以處理與核證機關的運作有關的風險，並須實施可應付以下事故（但不限於以下事故）的風險管理計劃：

a. 密碼匙資料外洩；

b. 核證機關的系統或網絡被入侵；

c. 核證機關的基建設施無法使用；及

d. 虛假製造證書及暫時吊銷和撤銷證書的資料。

4. 儲存庫

4.1 儲存庫

4.1.1 認可核證機關必須維持一個或多於一個經署長認可的儲存庫。

4.2 穩當可靠

4.2.1 認可核證機關必須以一個穩當系統維持認可儲存庫。

4.2.2 認可核證機關為維持認可儲存庫所進行的工作，不得對倚據認可證書或認可儲存庫所載資料的人士造成不合理的風險。

4.2.3 認可核證機關必須制訂全面的保安事故報告和處理程序及運作復原體系和程序，以維持認可儲存庫。

4.3 運作

4.3.1 認可核證機關的認可儲存庫必須包括載有以下資料的資料庫：

a. 在儲存庫公布的認可證書；

b. 由認可核證機關所公布有關認可證書被暫時吊銷或撤銷的通知；

c. 關於該認可核證機關的核證機關披露紀錄；

d. 署長就對該核證機關作出的認可所公布的一切命令或勸諭性聲明；及

e. 署長所指定的其他資料。

4.3.2 認可儲存庫不得載列虛假、不確或並非合理可靠的資料。

4.3.3 認可核證機關必須在認可儲存庫內把在至少過去七年內被暫時吊銷、撤銷或有效期屆滿的認可證書存檔。

5. 修訂業務守則

5.1 署長可不時修訂本業務守則，並將修訂通知根據條例第 20 及 28 條而獲得認可的核證機關。