粵港電子簽名證書互認證書策略

版本序號：1.0

工信部的對象標識符爲: 2.16.156.339.1.1.1.2.1 (自然人) / 2.16.156.339.1.1.2.2.1 (法人)

香港資科辦的對象標識符爲: 2.16.344.8.2.2008.810.2.2012.1.0 (繁簡體版本使用同一對象標識符)

生效日期: 2012 年 8 月 10 日

粵港電子簽名證書互認證書策略

版本序號：1.0

目錄

工信部的對象標識符爲：2.16.156.339.1.1.1.2.1（自然人）/ 2.16.156.339.1.1.2.2.1（法人）
香港資科辦的對象標識符爲：2.16.344.8.2.2008.810.2.2012.1.0（繁簡體版本使用同一對象標識符)

一、適用證書範圍

（一）本證書策略是核准由依據《中華人民共和國電子簽名法》獲得電子認證服務許可並在廣東省註冊登記的第三方電子認證服務機構或依據香港特別行政區《電子交易條例》成立的認可核證機關（以下統稱為電子認證服務機構）簽發的電子簽名證書或認可數碼證書（以下統稱電子簽名證書）能否應用於粵港跨境電子交易的重要依據。

（二）本證書策略主要適用於粵港跨境電子交易使用的個人電子簽名證書和組織機構電子簽名證書（以下簡稱為“個人證書”和“組織機構證書”，或統稱為“證書”）。本證書策略亦適用於簽發上述證書的電子認證服務機構本身的證書（以下簡稱為“電子認證服務機構本身的證書”）。

（三）本證書策略在規範簽發上述證書的電子認證服務機構行為基礎上，對規範證書持有人（以下簡稱為“訂戶”）、證書依賴方（以下簡稱為“依賴方”）等參與方行為亦提出明確要求。

二、規範範圍

本證書策略對電子認證服務機構有關證書的服務和管理提出以下規範性要求：

* 信息發布；
* 身份標識與鑒別；
* 證書生命週期操作要求；
* 認證機構設施、管理和操作控制；
* 認證系統技術安全控制；
* 證書和證書吊銷列表的描述；
* 合規性；
* 賠償限額、賠償安排和法律解決；
* 信息保密。

三、總體責任

（一）電子認證服務機構（包括其註冊機構）須[1]承擔以下責任，包括但不限於：

* 制定符合本證書策略要求的電子認證業務規則，依據本證書策略的要求及相關電子認證業務規則的條款，提供認證服務和相關的基礎設施；

[1] 在本證書策略中，“須”和“應”也是表示“必須”的意思。

* 電子認證服務機構須建立和執行符合相關規定的安全機制，保證私鑰得到安全的存放和保護；

* 所有和認證業務相關的活動須符合本地法律法規和主管部門的規定。

（二）電子認證服務機構須對證書訂戶承擔以下責任，包括但不限於：

* 證書中沒有電子認證服務機構所知的或源於電子認證服務機構的錯誤陳述；

* 生成證書時，不因電子認證服務機構的失誤而導致證書中的信息與電子認證服務機構所收到的信息不一致；

* 簽發給訂戶的證書符合本證書策略及相關電子認證業務規則的要求；

* 將按本證書策略及相關電子認證業務規則的規定，及時吊銷證書；

* 將向訂戶通報任何已知的、將在根本上影響證書有效性和可靠性的事件。

（三）電子認證服務機構須對依賴方（按照本證書策略及相關電子認證業務規則合理地依賴簽名（該簽名可通過證書中所含的公鑰驗證）的人）承擔以下責任，包括但不限於：

* 除未經驗證的訂戶信息外，證書中或證書指向的所有信息都是準確的；

* 完全遵照本證書策略及相關電子認證業務規則的規定簽發證書；

* 通過公開發布證書，向所有合理依賴證書中信息的依賴方證明：發證機構已向訂戶簽發了證書，並且訂戶已按照本證書策略及相關電子認證業務規則的規定接受了該證書。

四、信息發布

（一）信息庫

1、電子認證服務機構建立和維護一個或多個可公開查詢的在線信息庫，用於發布：

* 證書策略、電子認證業務規則及相關披露文檔等信息；

* 證書和證書狀態查詢（包括但不限於證書目錄信息、證書狀態信息、證書吊銷列表）等信息；

* 可公開的訂戶協議和必須公開的依賴方協議的最新版本；

* 本地主管部門指明必須發布的其他信息。

2、電子認證服務機構應在電子認證業務規則中清楚指出證書狀態信息的發布方式。證書狀態可以通過電子認證服務機構網站發布證書吊銷列表，也可以通過 LDAP 目錄服務器、OCSP 服務器作為證書吊銷列表的有效補充。

3、電子認證服務機構須根據 RFC3647 標準（或相關更新版本）制定電子認證業務規則的內容範

圍。若有不適用於該電子認證服務機構或某類型、類別或種類的證書範圍時，電子認證服務機構須在電子認證業務規則中清楚指出不適用的範圍及其原因。

4、電子認證服務機構須通過信息庫發布信息讓證書的依賴方清楚知道，在依賴方信賴電子認證服務機構簽發的證書時，必須對證書的使用承擔以下的主要責任，包括但不限於：

* 依賴方已經熟悉本證書策略及相關電子認證業務規則的條款，了解證書的使用目的和可提供的保證，依賴方在信任證書前，須同意依賴方協議中的條款，並根據使用的環境和條件判斷該證書是否可信任；

* 如果依賴方需要電子認證服務機構提供額外的保障，即電子認證業務規則中有關條款所提供的額外保障，依賴方應在確認可以獲得這些保障之後，自行決定是否信任相應的證書；

* 依賴方對證書進行合理的檢查和審核，包括檢查電子認證服務機構公佈的最新的證書吊銷列表，確認該證書沒有被掛起或吊銷；檢查證書信任路徑中所有出現過的證書的可靠性；檢查證書的有效期；檢查其它能夠影響證書有效性的信息；

* 依賴方在電子認證業務規則中的其他合理責任；

* 依賴方須承擔因未履行以上責任所產生的法律責任。

5、電子認證服務機構在電子認證業務規則及其它相關文檔中須清楚指出其信息庫的位置和查詢方式，以便能讓有關人士查詢並獲取所需信息，尤其是證書訂戶和依賴方對電子認證業務規則、證書及證書狀態的查詢。

6、電子認證服務機構須採取有效安全的措施防止信息庫受到未經授權的增加、刪除、修改等，且在運行及管理信息庫時，不得進行任何對依賴信息庫（包括證書和其他信息）的人士造成不合理風險的活動。

7、電子認證服務機構須在其與本證書策略相關的電子認證業務規則中聲明，在遵守本地法律監管要求和本證書策略的基礎上，任何由於電子認證服務機構或相關證書的不足或疏忽所引起的責任和索償，電子認證服務機構、訂戶和依賴方對兩地政府和電子認證服務主管部門免責。

（二）電子認證服務機構信息發布

8、電子認證服務機構在其信息庫中須公佈以下證書信息，包括但不限於：

* 電子認證服務機構本身的證書，其中包含與電子認證服務機構用作簽發證書的私鑰所對應的公鑰；

* 電子認證服務機構本身或其主管部門對電子認證服務機構本身的證書進行掛起、吊銷或不獲續期的通知；

* 任何對電子認證服務機構發出的證書的可靠性或服務能力造成重大及不利影響的事件。

（三）發布時間或頻率

9、電子認證服務機構須及時發布及更新信息庫中有關披露文檔和文檔的修訂信息，包括但不限於：

* 證書策略；
* 電子認證業務規則；
* 使用電子認證服務機構有關證書服務所需要的相關文檔；
* 電子認證服務機構上述文檔以往發布、修訂信息的披露記錄。

10、電子認證服務機構簽發的證書和相關信息，必須在生效後及時發布，以供下載、查詢和使用。

11、電子認證服務機構應發布證書（包括電子認證服務機構本身的證書）掛起或吊銷的信息（包括證書吊銷列表和任何其他有關掛起或吊銷的信息）。

* 當證書被掛起或吊銷時，電子認證服務機構應及時發布有關信息；
* 當證書被掛起或吊銷時,電子認證服務機構應及時發布有關的證書吊銷列表；
* 電子認證服務機構應至少每 24 小時發布一次證書有關的證書吊銷列表；
* 當電子認證服務機構本身的證書被掛起或吊銷時，電子認證服務機構應及時發布有關信息；
* 當電子認證服務機構本身的證書被掛起或吊銷時,電子認證服務機構應及時發布有關的證書吊銷列表；
* 電子認證服務機構應至少每年簽發一次電子認證服務機構本身證書有關的證書吊銷列表；
* 電子認證服務機構應在合理時間內發布證書吊銷列表，並在其相關的電子認證業務規則中清楚指出其證書吊銷列表的發布時間。

12、電子認證服務機構不應在其信息庫中載有已確認為不正確或不可靠的信息。

五、身份標識與鑒別

（一）證書上的身份命名

電子認證服務機構應在其簽發的證書保證:

1、證書在主體名稱 (subject name)中包含一個 X.501 甄別名(Distinguished Name (DN)) ，且按照 X.500 的解釋作為不同命名的規則。

2、訂戶的命名一定要有意義，應具有通常能夠被理解的語義，可以明確確定證書主體中的個人或者組織機構的身份，能夠把名稱與唯一一個確定的實體（個人或者組織機構）聯繫起來。當出現相同的名稱時，電子認證服務機構應有明確制度決定申請者的優先使用順序。證書不允許使用匿名或假名。個人證書的證書主體應以個人身份命名；組織機構證書的證書主體應以組織機構身份命名。

3、電子認證服務機構應要求證書申請者確保不會使用任何侵犯知識產權的名稱。電子認證服務機構應要求證書申請者當其申請的證書內容包含商標信息時，應提交有關的商標註冊文件，例如由政府機構發出的合法性證明文件。

（二）初次申請證書時的身份鑒別

4、組織機構身份的鑒別：

當任何組織機構（政府機構、企事業單位或其它社會組織等）提出證書申請時，電子認證服務機構應當先對其身份進行嚴格的鑒別，包括但不限於：

* 由獨立、權威的第三方提供的資料證明該組織確實存在，例如由政府機構發出的合法性證明，或由其它被認可的權威組織提供的證明資料；

* 通過有效方式確認組織機構申請資料的真實性，確保申請已得到該組織機構充分的授權並能提供其它必須驗證的信息；

* 申請的組織機構證書包括個人身份名義時，電子認證服務機構應要求該組織機構核實確認個人身份的真實性，並要求提交有關材料進行審核；

* 申請的組織機構證書由授權代表申請時，電子認證服務機構應要求授權代表提交該組織機構充分授權的書面證明文件（如授權書），審核確認授權代表得到該組織機構的明確授權；

* 以面對面的審核方式確認授權代表身份時，通過法定的身份證明文件（包括但不限於身份證、護照或者其它相身份證明資料），確認授權代表的真實身份；

* 在合理情況下使用認為必須的其它額外鑒別方式和資料。

5、個人身份的鑒別：

當個人提出證書申請時，電子認證服務機構應先對其身份進行嚴格的鑒別：

* 以面對面的審核方式確認個人身份時，通過法定的身份證明文件（包括但不限於身份證、護照或者其它身份證明資料），確認個人的真實身份，且其身份必須與所申請的證書主體相對應；

* 在合理情況下使用認為必須的其它額外鑒別方式和資料。

6、電子認證服務機構須在與某類型、類別或種類的證書對應的電子認證業務規則內清楚指出所採用的組織或個人身份鑒別方法（包括是否採用面對面的審核方式等）。

7、當證書上存在未經明確的、可靠驗證的訂戶信息時，電子認證服務機構須在電子認證業務規則及證書上清楚指出未經驗證的信息或信息類別。

（三）證書吊銷請求時的身份鑒別

8、電子認證服務機構須對證書吊銷請求進行合理的鑒別，包括但不限於以下程序：

* 當訂戶申請吊銷時，電子認證服務機構應要求訂戶提交與證書申請時相同的身份資料或利用原證書提交合法有效的電子簽名的吊銷申請，並對訂戶進行身份鑒別。申請者由於條件限制無法進行現場身份鑒別時，電子認證服務機構或其註冊機構應通過合理的方式，例如通過電話、郵遞、其他第三方的證明等，對申請者的身份予以鑒別驗證。當司法機關依法提出證書吊銷時，電子認證服務機構或其註冊機構可直接以司法機關書面的吊銷請求文件作為鑒別依據，不再進行其他方式的鑒別；

* 考慮到一般情況下，申請者的身份鑒別需要一定時間，不能即時吊銷證書，因此容許電子認證服務機構在合理情況下，可掛起證書，但仍應及時進行申請者的身份鑒別程序或處理司法機關書面的吊銷請求。

六、證書生命週期操作要求

（一）證書申請

1、電子認證服務機構（包括其註冊機構）可接受下列證書申請：

* 任何組織機構（政府機構、企事業單位或其它社會組織等）；
* 任何組織機構（政府機構、企事業單位或其它社會組織等）的授權代表；
* 個人申請者本人。

組織機構、授權代表和個人申請者的身份必須符合本策略的身份鑒別要求。

2、電子認證服務機構須要求所有證書申請者應在證書申請的過程中，

* 清楚了解及同意訂戶協議的內容，特別是關於責任和擔保的內容；
* 根據申請的證書類型提供真實、可靠、完整的身份資料；
* 承擔任何因提供虛假、偽造信息所產生的法律責任。

（二）證書申請處理

3、接受或拒絕證書申請:

電子認證服務機構在下列情況下，不應批准下述證書申請：

* 申請未能完全滿足本證書策略關於訂戶信息的標識和鑒別的規定；

* 申請者未能提供必需的身份證明材料或其他必須提供的支持文件；

* 申請者未能接受訂戶協議的內容和要求，特別是關於義務和擔保的內容。

4、電子認證服務機構須保留足以識別申請者身份的文檔記錄。

5、證書申請的處理期限：

電子認證服務機構必須在電子認證服務規則中明確規定處理時間，並且在承諾的處理時間內完成證書申請。

（三）證書簽發

6、電子認證服務機構接受申請者的證書申請後，基於對其證書申請文件進行審核和對申請人的身份進行鑒別的結果，進行證書簽發。

7、電子認證服務機構在安全的環境下通過系統為訂戶製作訂戶證書（包括密鑰對）、以及將證書以安全的方式交給訂戶等過程，均須保證私鑰不受干擾。電子認證服務機構不應接受訂戶提供的私鑰，也不應接受訂戶的密鑰更新請求。

8、電子認證服務機構一旦簽發證書，即向任何合理依賴該證書的人或任何合理依賴該證書的公鑰所能核實的電子簽名的人士保證：

電子認證服務機構已按照相關法律法規、本證書策略和證書相關的電子認證業務規則簽發該證書。

9、電子認證服務機構應將已經簽發的證書及其他有關的信息發布到可以被公開查詢的信息庫中。

10、電子認證服務機構及其註冊機構均須記錄所有與發出證書有關的交易事項，包括日期和時間。

11、電子認證服務機構簽發證書後，電子認證服務機構應及時通知訂戶，並提供獲得證書的方式，以確保訂戶能通過合理方式獲得證書。

（四）接受證書

12、電子認證服務機構應在訂戶協議和電子認證業務規則中清楚說明構成訂戶接受證書的行為（例如訂戶接受了包含有證書的介質），並要求訂戶清楚知道和確認這些構成接受證書的行為。

（五）證書更新

13、電子認證服務機構簽發的每張證書須包含有效期，當證書到期時，訂戶須獲得一張更新的

證書以繼續使用該證書。

14、電子認證服務機構處理證書續期時須確保提出證書續期請求的人是被更新證書所標識的訂戶。

15、電子認證服務機構及其註冊機構均須記錄與證書續期有關的所有交易事項，包括日期和時間。

（六）證書變更

16、當證書包含的信息（除公鑰外）發生變化時，訂戶須重新辦理證書。電子認證服務機構應不予接受對已發出的證書的內容作出變更的申請。

（七）證書吊銷和掛起

17、如電子認證服務機構有合理理由相信其發出的證書已經不可靠，則無論訂戶同意與否，電子認證服務機構應掛起該證書。電子認證服務機構須在一段合理時間內完成有關證書可靠性的調查，以及決定是恢復該證書的有效性或是吊銷該證書。如電子認證服務機構在考慮所有可取得的信息後，認為應即時吊銷其發出的證書的，則無論訂戶同意與否，電子認證服務機構須吊銷該證書。電子認證服務機構須在其電子認證業務規則中說明，若未能聯絡訂戶時應採取的行動。

18、電子認證服務機構須提供熱線電話或其他方式，以供訂戶向電子認證服務機構報告有關影響其證書或私鑰的事件，例如密鑰遺失或密鑰資料外泄等。

19、電子認證服務機構收到吊銷請求後，須驗證申請者的身份、權限和吊銷理由的正當性，確認無誤後方可進行吊銷。電子認證服務機構須在其電子認證業務規則明確自接到吊銷請求到完成吊銷的時限，任何掛起證書的處理不得超過合理的時限。電子認證服務機構須在有關的電子認證業務規則中清楚指出有關時限，並應力求不超過一個工作日。所有非經訂戶提出的吊銷請求，必須通過嚴格的內部程序並經由指定管理人員審批。當電子認證服務機構掛起或吊銷所發出的證書時，須在合理時間內通知該證書的訂戶。

20、電子認證服務機構必須嚴格控制由於證書製作過程中的失誤（例如證書下載錯誤、密鑰對不匹配）而導致證書吊銷。

21、證書被吊銷後，電子認證服務機構應在 24 小時內發布吊銷信息，包括使用證書吊銷列表和其他已公開的證書狀態查詢渠道（如適用）。電子認證服務機構應在電子認證業務規則中明確具體的吊銷信息更新時間。

22、當電子認證服務機構的密鑰（包括本身或子電子認證服務機構的密鑰）的安全被損害或者懷疑遭受損害時，電子認證服務機構應在合理的時間內採用適當的方式及時通知訂戶和依賴方。

23、電子認證服務機構必須對證書吊銷過程進行適當的記錄。

24、電子認證服務機構本身的證書吊銷請求，必須經過相關監管部門確定後才可以進行。

（八）密鑰對和證書的使用

25、電子認證服務機構須要求所有訂戶必須在簽訂訂戶協議和確認接受證書後，才能使用證書對應的私鑰，並要求訂戶確認一旦接受電子認證服務機構簽發的證書，訂戶即須承當如下責任：

* 訂戶私鑰的使用應符合證書中“密鑰用途”（KeyUsage）的要求；
* 訂戶私鑰和證書的使用應符合訂戶協議的要求；
* 訂戶在使用證書的公鑰所對應的私鑰進行電子簽名時，即保證是以訂戶的名義進行電子簽名，並且在生成電子簽名時，應已確保該證書沒有過期或被吊銷(若證書已到期或被吊銷，訂戶應停止使用私鑰)；
* 訂戶應保持對其私鑰的控制，並採取合理的措施來防止私鑰的遺失、洩露、被篡改或未經授權被使用；
* 訂戶不允許將證書用於非法活動；
* 訂戶應承擔訂戶協議中的其他責任。

（九）證書狀態服務

26、電子認證服務機構必須力求證書狀態服務維持 7*24 小時不間斷可用，儘量減少服務中斷時間。電子認證服務機構須在其電子認證業務規則中列出證書狀態服務不間斷可用和服務中斷時間的安排。證書狀態服務如需中斷（在安排下或不可預知或非電子認證服務機構能控制的情況下），電子認證服務機構必須儘量減少服務中斷時間。電子認證服務機構應確保可預先安排的證書狀態服務中斷時間每星期不得超過兩小時。電子認證服務機構應按本地監管要求，就服務中斷事項通知有關各方。

（十）終止證書服務/訂購的結束

27、電子認證服務機構須向訂戶和依賴方（包括在電子認證業務規則中）說明什麼情形下代表該訂戶的證書服務已經終止或訂購結束，包括但不限於下列情況：

* 在證書有效期內，證書被電子認證服務機構吊銷；
* 在證書到期前提出終止服務的申請，並獲電子認證服務機構接受；
* 證書有效期滿，沒有進行證書更新或密鑰更新。

28、電子認證服務機構應明確有關證書訂購結束的規定，制定證書訂購結束的具體實施流程，並妥善保存記錄。

（十一）密鑰託管與恢復

29、電子認證服務機構應在其電子認證業務規則中，明確密鑰託管和恢復服務的具體實施流程。

30、電子認證服務機構本身的密鑰不能被託管，訂戶的簽名密鑰也不能被託管。

七、認證機構設施、管理和操作控制

（一）物理安全和環境控制

1、電子認證服務機構須採取有效的物理安全控制措施：

* 識別及界定安全區域（例如有效區分公共區、服務區、管理區、核心區、屏蔽區等），根據不同區域的物理安全要求，採取有效的物理安全控制措施以確保該區域的物理安全；

* 制定電子認證服務機構職員及訪客進入該範圍的正規程序，並設立適當的安全控制措施（包括進入保安範圍的監察機制）；

* 須對影響儲存物理安全設備的地方加以特別保護；

* 對每一級物理安全層的訪問都必須是可審計和可控的，從而保證每一級物理安全層的訪問都只有獲授權的人員才可以進行；

* 具備機房環境監控系統，對基礎設施設備、機房環境狀況、安防系統狀況進行 7*24 小時實時監測，監測記錄保存時間應滿足故障診斷、事後審計的需要；電子認證服務機構須在其電子認證業務規則中指明監控記錄的保存時間，並至少保留 3 個月；

* 門禁系統應有進出時間記錄和超時報警提示，電子認證服務機構須定期對記錄進行整理歸檔；電子認證服務機構須在其電子認證業務規則中明確進出時間記錄的保存時間，並至少保留 3 個月；

* 確保只有授權人員才能操作電子認證服務機構的物理設備，並應針對不同安全級別的物理設備採取不同程度的訪問控制措施，包括但不限於：

  ① 授權人員須使用授權的口令登錄物理設備；

  ② 授權人員進入敏感區域時應有兩個因子以上的認證機制，其中一個因子應是生物特徵認證；

  ③ 確保設備訪問日誌不被篡改並進行定期檢查；

  ④ 需要至少兩個具有操作權限的人員來操作密碼模塊或者計算機系統；

  ⑤ 對高安全級別的物理設備進行 24 小時自動監視或者人工監視。

2、電子認證服務機構及其註冊機構的物理安全設施須配置主、備電力供應系統，以確保持續不間斷的電力供應。同時，也須有空調系統來控制溫度和濕度。

3、電子認證服務機構及其註冊機構應通過採取預防措施、採用相應的設備配置、制定相應的處

理程序來保護物理設施的安全，尤其應防止水災或者漏水對系統造成損害及其它不利後果。火災防護措施應當符合本地消防管理部門的要求。機房應設置火災自動報警系統和自動滅火系統，電子認證服務機構須在其電子認證業務規則中指明有否設置兩種火災探測器以檢測溫度和煙霧，火災報警系統應與滅火系統聯動。

4、電子認證服務機構及其註冊機構須嚴格保護備份系統數據及其它任何敏感信息的存儲介質，避免這些介質受到水災、火災、電磁以及因其它環境要素造成的損壞，並且須建立嚴格的保護手段以防止對這些介質被未經授權的使用、訪問或者披露。

5、電子認證服務機構及其註冊機構須建立嚴格的廢物處理流程，特別是包含隱私或者敏感信息的紙張、電子介質及其他任何廢棄物，保證對此類廢棄物進行徹底的物理銷毀或信息清除，避免這類廢物中包含的隱私或敏感信息被非授權使用、訪問或披露。

6、電子認證服務機構及其註冊機構須建立關鍵系統和數據（包括審計數據在內的任何敏感信息）的備份制度，對於關鍵系統和數據應採取異地備份手段以確保其處於安全的設施內。

7、凡電子認證服務機構依靠第三方提供服務以保障物理安全及環境控制的，該類服務須在該電子認證服務機構與第三方供應商訂立的正式服務協議內清楚說明。

8、電子認證服務機構的設施應受到保護，並避免受到自然災害影響。

9、電子認證服務機構應符合本地法律法規、監管條例、技術標準相關的其他適用要求（例如國家機房建設標準、消防條例等）。

（二）過程控制

10、電子認證服務機構應只容許被認定為可信的人員，才可在可信崗位上進行工作。可信崗位上的人員是指能夠訪問、進入或者控制證書或者密鑰操作的角色，可能會對以下幾個方面產生重要影響的人員，包括但不限於：

* 證書申請中的信息驗證和確認；
* 對證書申請、吊銷進行批准、拒絕或者其他操作；
* 證書簽發和吊銷；
* 對嚴格控制訪問的信息庫進行訪問；
* 處理訂戶信息或請求。

11、電子認證服務機構及其註冊機構須建立、維護和執行嚴格的控制流程，根據工作要求和工作安排採取職責分離措施，建立互相牽制、互相監督的安全機制，確保由多名可信人員共同完成敏感操作。須進行職責分離的角色，包括但不限於下列人員：

* 從事證書申請信息驗證的人員；

* 負責證書申請、吊銷、更新和信息註冊等服務請求的批准、拒絕或其他操作的人員；

* 負責證書簽發、吊銷等工作或者能夠訪問受限區域、敏感信息的人員；

* 處理訂戶信息的人員；

* 生成、簽發和銷毀電子認證服務機構系統證書的人員；

* 系統上線或者下線的人員；

* 掌握重要口令的人員；

* 密鑰及密碼設備管理、操作人員。

關鍵的控制須通過物理和邏輯的分割來實施，其中系統設備的邏輯和物理訪問等敏感操作應至少有 2 名可信人員參與。在電子認證服務機構的硬件密鑰設備的生命週期（從設備開始運作到邏輯/物理銷毀）過程中，對該設備的訪問應至少有 3 名可信人員共同參與。另外，一旦一個系統設備的密碼模塊被激活，進一步的邏輯或物理訪問必須實施職責分割。掌握系統設備的物理權限的人員不能再持有系統設備的秘密分割，反之亦然。

（三）人員安全

12、電子認證服務機構須制定有效的人員安全控制規定，並在有需要時更新。

13、對於所有將要在可信崗位上工作的人員，電子認證服務機構必須進行嚴格的身份識別和考核，確保其能夠滿足所從事的工作職責的要求，應：

* 根據實際需要確定不同的角色，劃分權限，設定不同角色的資歷和背景要求，並確保人員符合相應要求；

* 對人員進行安全審查（包括但不限於對被調查人的身份進行當面核查、要求被調查人提供有效身份證件）；

* 根據工作性質和職位權限的情況，賦予在可信崗位上工作的人員在系統和物理環境中的權限，採用合適的訪問控制技術（包括但不限於用於身份識別的系統操作卡、門禁卡、登錄口令、操作證書、作業帳號等安全令牌），以完整地記錄該人員所有敏感的操作行為；

* 在員工合同內加入與安全相關的條款。

14、電子認證服務機構須確保其所有人員（包括充當可信角色的人員）具備所需的技術資格和專業知識，以便能夠有效地履行職責，同時須為其員工提供適當及足夠的培訓（核心崗位至少每年一次），以確保他們執行任務的能力和安全策略得以有效的推行和遵守。培訓的內容可包括但不限於：

* 適當的技術培訓；

* 規章制度和程序；

* 處理安全事故及通知高層管理人員有關重大安全事故的程序。

15、電子認證服務機構須制定適當的控制措施以考察人員的表現，例如：

* 定期進行的工作績效考核；

* 正規的紀律程序（其中包括如何處置未獲授權的行為）；

* 正規的終止服務程序。

（四）事件紀錄程序/審計流程

16、電子認證服務機構須備存足夠的事件紀錄存檔，包括保留與該電子認證服務機構發出及管理的證書的有關文件，並須定期（不少於每個月一次）檢查事件紀錄，就任何異常情況採取適當行動。

17、電子認證服務機構須備存紀錄所有主要事件，包括但不限於：

* 對用於產生密鑰的資料及設備的訪問；

* 密鑰及證書的產生、發出、分派、儲存、備份、掛起、吊銷、撤回、存檔、銷毀及其他有關事項；

* 安全事件，包括但不限於密鑰資料洩露、網絡入侵等；

* 密碼設備的採購、安裝、使用、解除運作及棄用；

* 計算機設施的開發和運維記錄。

18、電子認證服務機構應保存原始審計日誌至少兩個月，並定期檢查審計日誌，以便發現重要的安全事件和管理問題，對發現的事件或問題應採取相應的措施，並對調查或審計行為進行記錄備案。電子認證服務機構應當採取嚴格的物理和邏輯訪問控制措施，防止所有的審計日誌和記錄被未經授權的瀏覽、修改、讀取、刪除等。電子認證服務機構應當建立和執行可靠的審計日誌備份制度，定期進行備份（至少兩個月備份一次），並在其電子認證業務規則中對備份週期進行明確規定。

19、電子認證服務機構應按照本證書策略的要求，對所有審計日誌的記錄進行歸檔。歸檔後原記錄應保存至少 5 年，或根據本地相關的法律法規要求，以較高的期限為準。

（五）記錄歸檔

20、電子認證服務機構除紀錄事件的規定外，還須對其他所有的重要記錄進行歸檔保存，重要記錄包括但不限於：

* 證書系統建設和升級文檔；

* 證書和證書吊銷列表；

* 證書申請支持文檔，證書服務批准和拒絕的信息，與證書訂戶的協議；

* 審計記錄；

* 證書策略、電子認證業務規則文檔；

* 員工資料，包括但不限於背景調查、錄用、培訓等資料；

* 各類外部、內部評估文檔。

21、不同歸檔記錄的保留期限可能是不同的，電子認證服務機構須根據法律法規的要求、業務需要和運營服務的實際情況，制訂不同歸檔記錄的保留期限，但自證書期滿或吊銷之日起，各種歸檔記錄應至少保存五年。

22、電子認證服務機構必須保留歸檔記錄的準確時間信息，包含記錄產生的日期和時間。

23、電子認證服務機構須採取適當的物理和邏輯訪問控制措施，保證只有獲授權的可信人員才能訪問所有歸檔的記錄。電子認證服務機構應將受保護的歸檔記錄保存在可靠的系統或者場所內，以防止受保護的歸檔記錄被進行未經授權的瀏覽、修改、刪除等非法操作。電子認證服務機構應保證歸檔記錄在保留期內可以被有效的訪問，並只有獲授權的可信角色人員能夠訪問歸檔記錄。歸檔時，電子認證服務機構應對歸檔記錄的一致性進行驗證。歸檔期間，電子認證服務機構必須驗證所有被訪問的記錄（通過適當的技術或方法）的一致性。

24、電子認證服務機構應定期對系統生成的電子歸檔記錄進行備份，並對備份文件實行異地存放。若沒對書面的歸檔資料進行備份，電子認證服務機構須採取嚴格的措施保證其安全性。

（六）事故處理、緊急應變、災難恢復及業務持續

25、電子認證服務機構須為包括所有關鍵運營範圍內可能發生的重大事故，制定事故處理、緊急應變、災難恢復和業務持續運作的程序和應對措施以保證應有的服務水平（包括證書狀態查詢服務應參照本證書策略第六章“證書生命週期操作要求”第九點“證書狀態服務”的要求；其他證書核心服務如證書掛起服務、證書吊銷服務等，應指明中斷時間），並適時進行維護及更新。可能發生的重大事故包括但不限於：

* 計算機資源、軟件、數據出現損壞或重大故障的事件（包括影響外部訪問信息庫的事件）；

* 註冊機構因事故終止服務；

* 電子認證服務機構或其子電子認證服務機構私鑰出現損毀、遺失、洩露、被破解、被篡改，或者有被第三者竊用的懷疑時。

26、電子認證服務機構應定期對災難恢復和業務持續運作的應對措施進行演練，並對演練程序和結果進行記錄。應對措施中所包括的有關主要人員均須參與演練。

八、認證系統技術安全控制

（一）密鑰對生成和安裝

1、電子認證服務機構須制定和採取有關生成密鑰對的操作控制措施，包括但不限於：

* 用以確保產生密鑰對設備完整無誤的程序；

* 用以確保密鑰對是由獲授權人員在受到嚴密控制的方式下生成的程序。

2、當電子認證服務機構為訂戶生成密鑰對後，電子認證服務機構應通過安全的途徑、以防篡改封裝的方式將私鑰分發給訂戶。用於存儲證書（包括私鑰）的介質技術應符合《粵港兩地電子簽名證書互認技術標準列表和採用措施》內的規定(附件 1.2），電子認證服務機構須在電子認證業務規則中指明存儲訂戶證書私鑰的介質技術。分發訂戶私鑰和激活私鑰的數據應採用不同的途徑發給訂戶，電子認證服務機構應對每次私鑰分發進行記錄。

3、電子認證服務機必須在符合本地安全、本地監管要求和本策略要求的硬件設備條件下生成用於簽發證書和證書狀態信息的密鑰對。

（二）電子認證服務機構密鑰變更

4、電子認證服務機構應適時更新其本身的證書和密鑰對，保證其本身的證書鏈和密鑰對可順利過渡，力求減少對訂戶和依賴方的影響。

5、電子認證服務機構更替其密鑰對時，電子認證服務機構必須保證整個證書鏈的順利過渡。

（三）私鑰保護和密碼模塊工程控制

6、電子認證服務機構應保證產生密鑰的密碼模塊的安全標準符合《粵港兩地電子簽名證書互認技術標準列表和採用措施》內的規定（附件 1.2）。

7、電子認證服務機構須在其與某類型、類別或種類的證書對應的電子認證業務規則中清楚指出所採用的所有相關密碼算法技術標準。

8、電子認證服務機構須就產生密鑰的工具的採購、接收、安裝、驗收測試、調試、使用、維修、保養及棄用等制定有效的程序及控制措施，包括但不限於：

* 制定有效程序，以確保密碼模塊的完整性；

* 制定有效程序，以確保產生密鑰的工具由獲授權的人員在適當的督導下操作，防止工具遭擅自改動；設立控制機制，以確保密碼模塊不會在不能偵測的情況下被擅自改動；

* 制定有效程序，以確保使用密碼模塊產生的密鑰的強度，是符合電子認證服務機構及訂戶使用密鑰的目的所需的適合強度，也符合《粵港兩地電子簽名證書互認技術標準列表和採用措施》（附件 1.2）內關於電子簽名有關密碼算法的規定；

* 制定有效的程序及控制措施，以確保在不同密碼模塊之間傳輸密鑰時，不會發生私鑰丟失、失竊、洩露、被篡改或者未經授權的被使用；

* 電子認證服務機構的私鑰需要在密碼模塊中以加密方式保存。

9、電子認證服務機構應對任何用於存儲密鑰的存儲介質（如智能卡）的預備、啟動、使用、分派及終止使用制定有效的程序及控制措施。

10、電子認證服務機構的私鑰操作應採用多人控制（M 選 N 多人控制（M>N>1））的策略，使用“秘密分割”技術，將使用和操作電子認證服務機構私鑰時所需的激活數據分成若干部分，由獲管理層授權的可信人員持有，並在對私鑰進行操作時，共同完成生成和分割程序。電子認證服務機構須以安全的方式分開保存機構本身的私鑰及其激活數據。

11、電子認證服務機構必須以安全的方式對電子認證服務機構私鑰進行備份，並根據備份災難恢復操作需要，以安全的設備和方式保管私鑰備份。

12、電子認證服務機構私鑰生命期結束後，電子認證服務機構應遵從本證書策略關於歸檔的規定，採取安全保密方法進行保存。歸檔期限結束後，電子認證服務機構對機構私鑰的銷毀應符合本證書策略關於私鑰銷毀的規定。

13、電子認證服務機構須制定能夠確保安全銷毀密鑰對及任何有關設施的控制措施，包括採取足以確保銷毀私鑰的所有備份的程序（確保私鑰在銷毀後再不能被復原或重組），以及吊銷對應的證書的程序。

（四）密鑰對管理的其他方面

14、電子認證服務機構須對本機構所有的公鑰進行歸檔。

15、電子認證服務機構應遵守以下證書操作週期和密鑰對使用期限的要求，包括但不限於：

* 證書操作週期應於過期或被吊銷後終止；

* 訂戶密鑰對的使用週期與證書的操作週期應是相同的；僅在簽名驗證時，證書操作週期結束後密鑰對的公鑰還可以繼續使用；

* 電子認證服務機構所簽發的證書的操作週期應不得超過電子認證服務機構密鑰對的使用週期；

* 用於身份鑒別的證書，其密鑰對只可以在證書有效期內使用；僅在簽名驗證時，證書操作週期結束後密鑰對的公鑰還可以繼續使用；

* 訂戶證書有效期應指明最長不得超過 5 年。電子認證服務機構本身的證書應指明最長的有效期不得超過 50 年。

16、電子認證服務機構必須保證所有生成和安裝激活數據的程序是安全可靠的，從而避免私鑰被洩漏、被偷竊、被非法使用、被篡改、或者被非經授權的披露。

（五）計算機和網絡安全控制

17、電子認證服務機構應制定全面、完善的安全管理策略和制度，通過嚴格的安全控制手段，確保電子認證服務機構軟件和存儲數據文件的系統是安全、可信賴的系統，不會受到未經授權的內部和外部訪問。

18、電子認證服務機構應建立嚴格的管理體系來控制和監視運行系統，以防止未授權的修改。

19、電子認證服務機構應採用多級防火牆、入侵檢測、安全審計、病毒防範系統等措施來保護電子認證服務機構網絡環境的安全，適時更新版本，定期針對網絡環境進行風險評估和審計，以檢測有否被入侵的危險，盡可能降低來自網絡的風險。

20、電子認證服務機構處理廢舊設備時，必須清除影響認證業務安全性的信息存儲並加以確認。

21、電子認證服務機構應按照《粵港兩地電子簽名證書互認辦法》要求，定期聘請獨立第三方機構進行包括計算機和網絡安全在內的整體評估。

（六）系統開發控制

22、電子認證服務機構須制定系統開發、升級和維護工作的程序，採取有效的控制措施，並適時作出修改或更新。這些程序及措施的內容應包括但不限於：

* 無論由電子認證服務機構人員或在特殊情況下由其它機構進行開發工作，均能使用一致和有效的內部標準；
* 將生產及開發的環境分隔開的有效程序；
* 將操作、運維、開發人員的職責得以區分的有效程序；
* 對用於生產及開發的環境內的資料及系統進行有效訪問的控制措施；
* 對變更控制程序（包括但不限於系統和數據的正常和緊急變更）的有效控制措施（包括但不限於版本的控制、嚴格的測試驗證等）；
* 系統上線前進行安全性的檢查和評估的程序，檢查和評估內容包括有否安全漏洞和被入侵的危險等；
* 對採購設備及服務進行妥善管理的有效程序。

（七）時間戳

23、電子認證服務機構應保證各種系統日誌、操作日誌有準確的時間標識。

九、證書和證書吊銷列表的描述

1、電子認證服務機構應保證證書所採用的技術和證書結構符合《粵港兩地電子簽名證書互認辦法》和《粵港兩地電子簽名證書互認技術標準列表和採用措施》（附件 1.2）內的規定。電子認證服

機構採用具體技術方案時應考慮證書跨境使用所需的互聯互通需求。

2、電子認證服務機構應根據《ITU X.509》（第三版）（ITU X.509 v3）的證書格式發出及管理公鑰證書，並根據《ITU X.509》（第二版）（ITU X.509 v2）的證書吊銷列表格式產生及公佈證書吊銷列表。

3、電子認證服務機構須在與某類型、類別或種類的證書對應的電子認證業務規則中清楚說明所採用的證書結構（包括證書擴展項）及所包含的技術標準（例如包括採用何種數字符代碼）。

4、如電子認證服務機構採用 OCSP 技術作為證書吊銷列表的補充，以方便證書訂戶和依賴方及時查詢證書狀態信息，電子認證服務機構須在其電子認證業務規則中具體說明操作方式、所提供的信息及使用的技術標準。

十、合規性

1、電子認證服務機構須建立和執行有效的內部審查程序，以確保其遵守所有適用的法律法規、本證書策略、對應的電子認證業務規則及其相關的內部規章制度。

2、電子認證服務機構須按照《粵港兩地電子簽名證書互認辦法》的要求以本證書策略為依據每年聘請獨立第三方機構進行執行審查。

3、對執行審查報告中提出的例外情況、不足之處或建議，電子認證服務機構須作出回應，並適時提交包括改善和預防措施的整改計劃書。

十一、賠償限額、賠償安排和法律解決

1、電子認證服務機構在向訂戶發出某類型、類別或種類的證書時，須在與該類型、類別或種類證書對應的有關電子認證業務規則中指明該證書的賠償限額，同時指明依據限額對使用該證書所代表的涵義和重要性。

2、電子認證服務機構須安排採購適當的保險或作出符合監管部門要求其他方式的賠償安排（例如賠償保證存款金），以確保該機構有足夠能力承擔因發出或使用證書而引起的或與此有關的潛在法律責任。為證書採購保險的電子認證服務機構應在其信息庫中發布有關保險的保險號或其他存在證據。當本地主管部門或獨立第三方機構在審查中提出要求時，電子認證服務機構應立即提交該保險號或上述保險的存在證據。

3、電子認證服務機構應承諾分別在訂戶協議及其電子認證業務規則中明確規定對訂戶和依賴方的賠償。

4、無論證書訂戶、依賴方等實體在何地居住以及在何處使用證書，本證書策略的執行、解釋和程序有效性均適用於簽發該證書的當地法律。電子認證服務機構須明確注明就本證書策略或電子認證業務規則所涉及的任何爭議可處理該爭議的法庭。

十二、信息保密

電子認證服務機構必須對保密信息（包括但不限於須保密的業務信息和個人隱私信息）承擔相應的保護責任，清楚界定受保護範圍，並通過有效的管理制度和技術手段對其進行保護。

十三、附則

1、本證書策略適用於根據《粵港兩地電子簽名證書互認辦法》參與粵港兩地電子證書互認機制的電子認證服務機構。

2、本證書策略由“粵港電子簽名證書互認工作組” 依據《粵港兩地電子簽名證書互認辦法》進行修訂。

3、本證書策略自《粵港兩地電子簽名證書互認辦法》發布日起實施和生效。

附件 1.1：互認策略主要名詞術語的兩地對照表

名詞術語	內地習慣用法	香港習慣用法	名詞解釋*
電子簽名證書	電子簽名證書 (electronic signature certificate)	數碼證書 (digital certificate)	以電子形式發出的證書，其所儲存的數據可用以核實證書擁有人的身份。證書通常包含的資訊包括用戶的公開密碼匙、姓名及電子郵件地址。
電子簽名	電子簽名	數碼簽署 (digital signature)	指數據電文中以電子形式所含、所附用於識別簽名人身份並表明簽名人認可其中內容的數據。
證書策略	證書策略	證書政策 (certificate policy)	一套命名的規則集，用以指明證書對一個特定團體和（或者）具有相同安全需求的應用類型的適用性。
電子認證服務機構	電子認證服務機構	核證機關 (certification authority)	指向個人或組織發出證書的機構。
電子認證業務規則	電子認證業務規則	核證作業準則 (certification practice statement)	關於電子認證服務機構在簽發、管理、吊銷或更新證書過程中所採納的業務實踐的聲明。
註冊機構	註冊機構	登記機關 (registration authority)	代表電子認證服務機構承擔某些任務的實體，但並不簽發證書。
私鑰	私鑰	私人密碼匙 (private key)	指對密鑰配中用作產生電子簽名的密鑰。
公鑰	公鑰	公開密碼匙 (public key)	指配對密鑰中用作驗證電子簽名的密鑰。

名詞術語	內地習慣用法	香港習慣用法	名詞解釋*
主體名稱	主體名稱	主體名稱 (subject name)	指證書持有者名字的信息。
甄別名	甄別名	甄別名 (distinguished name)	指證書裡唯一標識證書用戶的身份的信息。
訂戶	訂戶	登記人 (subscriber)	泛指被頒發一個證書的證書主體。
依賴方	依賴方	依賴方 (relying party)	證書的接收者，依賴於該證書和（或）該證書所驗證的電子簽名。
吊銷證書	吊銷證書	撤銷證書 (certificate revocation)	指電子認證服務機構終止證書的有效性。
掛起證書	掛起證書	暫時吊銷證書 (certificate suspension)	指電子認證服務機構令證書暫時失效。
證書吊銷列表	證書吊銷列表	證書撤銷清單 (certificate revocation list)	指由電子認證服務機構公佈的列表，列載其發出卻已被吊銷或掛起的證書。
賠償限額	賠償限額	倚據限額 (reliance limit)	指就證書的倚據而指明的金錢限額。
證書口令	證書口令	證書密碼 (certificate password)	指訂戶使用證書時所輸入的字符串。
工作績效考核	工作績效考核	工作表現評核 (performance assessment)	對電子認證服務機構工作人員在執行職務時的工作表現所作的系統化評審過程。

- 釋義僅作參考用途，所有名稱的定義應以兩地各自的法律法規、慣常定義或證書相關協議內容等所使用的定義為準。

附件 1.2：《粵港兩地電子簽名證書互認技術標準列表和採用措施》

相關技術範圍	兩地互認證書採用有關基本標準
證書格式	ITU X.509 V3 或 符合《GB/T 20518-2006 信息安全技術公鑰基礎設施　數字證書格式》
證書吊銷列表	ITU X.509 V2
信息庫	HTML, LDAP, HTTP
電子簽名有關密碼算法	第一類： • RSA, SHA-1 （未來將過渡至 SHA-2） • 證書和電子認證服務機構本身的證書：RSA 2048 位 或 第二類： • SM2、SM3
密碼模塊的安全標準	按本地監管部門批准的標準
數字證書介質技術	PKCS#11 兼容裝置 或 符合國家密碼管理局《智能 IC 卡及智能密碼鑰匙密碼應用接口規範》

電子簽名證書應載明的內容（根據《粵港兩地電子簽名證書互認辦法》）	
1、證書簽發機構名稱； 2、證書持有人名稱； 3、證書序列號； 4、證書有效期； 5、證書持有人的簽名驗證數據； 6、證書簽發機構的簽名； 7、證書策略對象標識符； 8、規定的其他內容。	
鼓勵（或要求）採用、跨境證書使用便利化的措施	
電子認證業務規則	鼓勵電子格式化（XML）和 PDF 文檔格式，雙語言（中、英語）； **要求有中文 PDF 文檔格式並以此為準**。
符合互認條件的證書“信任列表”（監管範圍）	鼓勵 HTML/PDF（人讀）和 XML（機讀）置放于安全網站上或其他合適的渠道; **要求有 HTML/PDF（人讀）文檔格式置放于安全網站上或其他合適的渠道，並以此為準**。