

立法院憑證管理中心
憑證實務作業基準

The Legislative Yuan
Certification Authority
Certification Practice Statement

第1.2版

立法院

中華民國一〇二年十一月一日

目 錄

1	簡 介	4
1.1	概 述	4
1.2	文件與識別	4
1.2.1	文 件	4
1.2.2	識 別	4
1.3	公開金鑰基礎建設參與成員	4
1.3.1	憑證中心	4
1.3.2	註冊中心	4
1.3.3	憑證用戶	4
1.3.4	信賴憑證者	5
1.3.5	其他參與成員	5
1.4	憑證適用性	6
1.4.1	適用範圍	6
1.4.2	限制範圍	6
1.5	政策管理	6
1.5.1	管理單位	6
1.5.2	聯絡窗口	6
1.5.3	憑證實務作業基準之審定	6
1.5.4	憑證實務作業基準審定程序	6
1.6	本文件相關定義與縮寫	7
2	一般條款	8
2.1	職責及義務	8
2.1.1	立法院之職責	8
2.1.2	憑證中心之職責	8
2.1.3	註冊中心之職責	8
2.1.4	憑證用戶之義務	8
2.1.5	信賴憑證者之義務	9
2.1.6	儲存庫服務之義務	9
2.2	法律責任	9
2.2.1	憑證中心之責任	9
2.2.2	註冊中心之責任	9
2.3	財務責任	10
2.3.1	憑證中心之賠償責任	10
2.3.2	註冊中心之賠償責任	10
2.3.3	憑證用戶之賠償責任	11
2.3.4	對憑證用戶及信賴憑證者之賠償責任	11
2.3.5	財務保險與財會稽核	11
2.4	解釋及施行	11

2.4.1	政府法令	11
2.4.2	適用性	11
2.4.3	仲 裁	11
2.5	費 用	11
2.5.1	憑證申請及更新費用	11
2.5.2	憑證查詢費用	11
2.5.3	憑證廢止及狀態查詢費用	11
2.5.4	退 費	12
2.6	公布與儲存庫	12
2.6.1	儲存庫	12
2.6.2	憑證中心之資訊公布	12
2.6.3	公布頻率	12
2.6.4	存取控制	12
2.7	稽 核	12
2.7.1	稽核的頻率	12
2.7.2	稽核者身分鑑別及資格	13
2.7.3	被稽核單位與稽核者關係	13
2.7.4	稽核範圍	13
2.7.5	對於稽核結果之因應方式	13
2.7.6	稽核結果查詢	13
2.8	機密及隱私	13
2.8.1	機密資訊種類	13
2.8.2	非機密資訊的種類	14
2.8.3	隱私權保護	14
2.9	智慧財產權	14
2.9.1	一般條款	14
2.9.2	著作權	14
3	識別及鑑別	15
3.1	命 名	15
3.1.1	命名種類	15
3.1.2	命名須有意義	15
3.1.3	憑證用戶之匿名與假名	15
3.1.4	命名形式之解釋規則	15
3.1.5	命名之獨特性	15
3.1.6	商標之辨識、鑑別及角色	16
3.2	初始驗證	16
3.2.1	證明擁有私密金鑰之方式	16
3.2.2	個人身分鑑別之程序	16
3.2.3	組織身分鑑別之程序	16

3.2.4	硬體裝置或伺服器軟體鑑別之程序	17
3.3	金鑰更換	17
3.3.1	憑證之金鑰更換	17
3.3.2	廢止憑證之金鑰更換	17
3.4	憑證廢止之識別與鑑別程序	17
4	營運規範	18
4.1	憑證申請	18
4.1.1	申請者	18
4.1.2	申請登記過程	18
4.2	申請憑證之程序	18
4.2.1	立法委員憑證	18
4.2.2	公費助理憑證	18
4.2.3	職員憑證	18
4.2.4	伺服器應用憑證	18
4.2.5	外包廠商憑證	19
4.2.6	外單位憑證	19
4.2.7	院內單位臨時憑證	19
4.2.8	傳播媒體憑證	19
4.3	簽發憑證之程序	19
4.3.1	憑證中心簽發憑證	19
4.3.2	憑證中心明確告知申請者	20
4.4	接受憑證之程序	20
4.4.1	接受憑證程序	20
4.4.2	憑證中心公布此憑證	20
4.5	金鑰對和憑證使用	20
4.5.1	用戶私鑰和憑證使用	20
4.5.2	可信賴用戶公鑰和憑證使用	20
4.6	憑證更新	21
4.6.1	憑證更新事由	21
4.6.2	憑證更新申請者	21
4.6.3	憑證更新請求	21
4.6.4	公告憑證更新給憑證用戶	21
4.6.5	已更新憑證的接受程序	21
4.6.6	憑證中心公布已更新憑證	21
4.6.7	憑證中心公告簽發憑證給其他單位	21
4.7	憑證金鑰更換	21
4.7.1	憑證金鑰更換事由	21
4.7.2	公鑰申請者	21
4.7.3	憑證金鑰更換請求	21

4.7.4	公告憑證簽發給憑證用戶	21
4.7.5	已更換憑證金鑰的接受程序	21
4.7.6	憑證中心公布已更換憑證金鑰	21
4.7.7	憑證中心公告簽發憑證給其他單位	21
4.8	憑證修正	22
4.8.1	憑證修正事由	22
4.8.2	憑證修正申請者	22
4.8.3	憑證修正更換請求	22
4.8.4	公告憑證修正給憑證用戶	22
4.8.5	已修正憑證的接受程序	22
4.8.6	憑證中心公布已修正憑證	22
4.8.7	憑證中心公告簽發憑證給其他單位	22
4.9	憑證廢止及暫時停用	22
4.9.1	憑證廢止之事由	22
4.9.2	憑證廢止之申請者	23
4.9.3	憑證廢止之程序	23
4.9.4	憑證廢止申請的處理期限	23
4.9.5	憑證中心處理憑證廢止時間	24
4.9.6	憑證廢止查驗之規定	24
4.9.7	憑證廢止清冊之簽發頻率	24
4.9.8	憑證廢止清冊之最大潛在因素	24
4.9.9	線上憑證狀態查詢服務	24
4.9.10	線上憑證狀態查詢之規定	24
4.9.11	其他形式廢止公告	24
4.9.12	金鑰被破解時之其他特殊規定	24
4.9.13	暫時停用憑證之事由	24
4.9.14	暫時停用憑證之申請者	25
4.9.15	暫時停用及恢復使用憑證之程序	25
4.9.16	暫時停用憑證的期間	25
4.9.17	暫時停用憑證的處理期限	26
4.10	憑證狀態查詢服務	26
4.10.1	查詢憑證運作特性	26
4.10.2	查詢憑證適用性	26
4.10.3	查詢憑證附加功能	26
4.11	簽發終止	26
4.12	金鑰託管與復原	26
4.12.1	金鑰託管與復原策略與實作	26
4.12.2	會議金鑰封裝與復原策略與實作	26
5	非技術性安全控管	27

5.1	實體管控	27
5.1.1	實體所在及結構	27
5.1.2	實體存取	27
5.1.3	電力及空調系統	27
5.1.4	水源干擾	27
5.1.5	防火設施	27
5.1.6	儲存媒介	27
5.1.7	廢棄物處理	27
5.1.8	異地備援	28
5.2	作業程序控管	28
5.2.1	信任規則	28
5.2.2	每項工作所需的人數	29
5.2.3	角色的識別與驗證	29
5.3	人員控管	29
5.3.1	適任條件與經歷	29
5.3.2	背景調查過程	29
5.3.3	教育訓練	29
5.3.4	職位調動的頻率及順序	29
5.3.5	未授權行動的制裁	29
5.3.6	約聘人員的規定、人事合約的需求	30
5.3.7	文件資料的提供	30
5.4	安全稽核程序	30
5.4.1	被記錄事件種類	30
5.4.2	處理紀錄的頻率	30
5.4.3	稽核紀錄保留期限	30
5.4.4	稽核紀錄的保護	31
5.4.5	稽核紀錄備份程序	31
5.4.6	安全稽核系統	31
5.4.7	對引起事件者之告知	31
5.4.8	弱點評估	31
5.5	紀錄歸檔方法	31
5.5.1	紀錄事件之類型	31
5.5.2	歸檔之保留期限	31
5.5.3	歸檔之保護	32
5.5.4	歸檔之備份程序	32
5.5.5	紀錄之時戳要求	32
5.5.6	歸檔資料彙整系統	32
5.5.7	歸檔紀錄之取得及驗證程序	32
5.6	金鑰更換	32

5.7	金鑰遭破解或災變時之復原程序	33
5.7.1	電腦資源、軟體、資料被竄改	33
5.7.2	金鑰憑證被廢止之復原程序	33
5.7.3	金鑰憑證遭破解之復原程序	33
5.7.4	安全設施之災後復原工作	33
5.8	憑證中心終止服務	33
6	技術安全控管	35
6.1	本憑證中心金鑰對之產製與安裝	35
6.1.1	金鑰對之產製	35
6.1.2	私密金鑰之安全遞送	35
6.1.3	公鑰遞送給本憑證中心	35
6.1.4	憑證中心公鑰傳送給憑證用戶	35
6.1.5	金鑰長度	35
6.1.6	公開金鑰參數的產生	35
6.1.7	參數品質的檢核	36
6.1.8	金鑰經軟體或硬體產製	36
6.1.9	金鑰之使用目的	36
6.2	私密金鑰的保護	36
6.2.1	標準密碼模組	36
6.2.2	私密金鑰的分持控管	36
6.2.3	私密金鑰的託管	36
6.2.4	私密金鑰的備份	36
6.2.5	私密金鑰的歸檔	37
6.2.6	私密金鑰輸入至密碼模組	37
6.2.7	私密金鑰的啟用	37
6.2.8	私密金鑰的停用	37
6.2.9	私密金鑰的回復	37
6.2.10	私密金鑰的銷毀	37
6.3	用戶金鑰對管理之其他規定	38
6.3.1	公開金鑰的歸檔	38
6.3.2	公開金鑰及私密金鑰的有效期限	38
6.4	啟動資料	38
6.4.1	啟動資料的產生與安裝	38
6.4.2	啟動資料的保護	38
6.4.3	啟動資料的其他考量	38
6.5	電腦安全控管	38
6.5.1	特定電腦安全技術需求	38
6.5.2	電腦系統安全等級	39
6.6	生命週期技術控管措施	39

6.6.1	系統開發控管措施	39
6.6.2	安全管理控管措施	39
6.6.3	生命週期安全等級	39
6.7	網路安全管控	39
6.8	密碼模組工程的管控	39
7	憑證及憑證廢止清冊的剖繪	40
7.1	憑證的剖繪	40
7.1.1	版本號碼	40
7.1.2	憑證擴充欄位	40
7.1.3	演算法的物件識別代碼	40
7.1.4	命名形式	41
7.1.5	命名限制	41
7.1.6	憑證政策物件識別碼	41
7.1.7	憑證政策限制擴充欄位的使用	41
7.1.8	憑證政策限定元的語法及語意	41
7.1.9	關鍵憑證政策擴充欄位的語意處理	41
7.2	憑證廢止清冊的剖繪	41
7.2.1	版別號碼	41
7.2.2	憑證廢止清冊與憑證廢止清冊的擴充欄位	41
8	憑證實務作業基準之維護	42
8.1	本作業基準之生效與終止	42
8.1.1	本作業基準之生效	42
8.1.2	本作業基準之終止	42
8.1.3	本作業基準之終止的影響	42
8.2	本作業基準之變更程序	42
8.2.1	變更時不另作通知之變更項目	42
8.2.2	應通知之變更項目	42
8.3	本作業基準之公布及通知程序	42
8.4	本作業基準之核准程序	42

摘 要

立法院(以下簡稱本院)遵循經濟部依據電子簽章法授權發布訂定之「憑證實務作業基準應載明事項準則」規定，制定本院憑證管理中心憑證實務作業基準(以下簡稱本作業基準)，重要事項說明如下：

1、主管機關核定文號：經濟部經商字第 09700608200 號

2、簽發之憑證種類、保證等級及適用範圍

(1)憑證種類

本院憑證管理中心(The Legislative Yuan Certification Authority, LYCA，以下簡稱本憑證中心)之用戶為本院委員、公費助理、職工同仁、聘僱人員、以及特殊專案申請者(包含外包廠商、媒體記者、本院卸任委員、退休職工人員或其他特殊使用者)等(以下簡稱憑證用戶)。本憑證中心所簽發之憑證除自簽憑證外，包含立法委員憑證、公費助理憑證、職員憑證、伺服器應用憑證、外包廠商憑證、外單位憑證、院內單位臨時憑證與傳播媒體憑證等八種公鑰憑證(以下均簡稱憑證)。

(2)保證等級

本憑證中心依據「立法院憑證管理中心憑證政策」(以下簡稱憑證政策)簽發簽章用及加密用之憑證，簽發之憑證均為相同之保證等級，該等級可應用於本院通訊網路或網際網路上之資訊應用業務；該等級保證簽署者身分的真實性及資料的完整性，同時做為電子文件之簽署及其鑑別。

(3)適用範圍

適用於本院相關應用服務所需之身分認證、加密與簽章。憑證用戶及信賴憑證者，必須謹慎使用本憑證中心所簽發之憑證，不得違反本作業基準第 1.4.1 章節所適用及第 1.4.2 章節所限制之範圍。

3、認證服務的第三人稽核

本憑證中心由本院依政府採購法，委外辦理本憑證中心之外部稽核作業，委託公正之第三人，就本憑證中心的運作進行稽核。

4、使用憑證之重要聲明

(1)憑證申請

憑證用戶向註冊窗口(請參考第 1.3.5(1)章節說明)申請憑證時，必須提供詳細且正確之身分證明文件與資料，確實了解並同意申請表上之權利與義務，以及憑證申請與使用的作業規範內容，並且於接受該規範的規定下始可簽名確認；憑證用戶因故意、過失或不正當意圖而提供不實資料，致造成他人遭受損害時，應由該憑證用戶負損害賠償責任。

(2)憑證使用

憑證用戶必須妥善保管與憑證相對應之私密金鑰與保護密碼，當有被冒用、曝露及遺失等不安全之顧慮時，或不再使用該憑證時，應於一個工作天內向註冊窗口辦理申告及處理；如因故意或過失，致造成他人遭受損害時，應由該憑證用戶負損害賠償責任。

憑證用戶必須依照本作業基準業務應用系統規範的規定，合法且正確地使用私密金鑰與憑證於相關業務。憑證用戶或信賴憑證者皆應依憑證內記載的適用範圍，使用於適用的業務範圍內。

5、法律責任

- (1)憑證用戶或信賴憑證者，如未依照本作業基準規定之適用範圍使用憑證，所引發之後果，本憑證中心不負任何法律責任。
- (2)憑證用戶或信賴憑證者因使用憑證，而發生損害賠償事件時，本憑證中心的損害賠償責任，則以本作業基準第 2.3 章節所規定之責任範圍為限。
- (3)如因不可抗力或其他非可歸責於本憑證中心之事由，所導致的損害事件，本憑證中心不負任何法律責任。
- (4)註冊中心與註冊窗口(請參考第 1.3.2 章節說明)因執行業務所引發的法律責任，除法令另有規定外，由本憑證中心負責。
- (5)如因憑證用戶隱瞞事實，提供註冊窗口不正確資料，導致信賴憑證者遭受損害時，如該損害之造成，不可歸責於註冊窗口時，應由憑證用戶自負損害賠償的責任；若憑證用戶隱瞞事實且註冊窗口有疏失時，除憑證用戶應負本作業基準第 2.3.3 章節規定之賠償責任外，註冊窗口應依公務人員服務相關規定辦理。
- (6)憑證用戶之憑證如須暫停使用、恢復使用或廢止，應依照本作業基準相關規定辦理；如發生私密金鑰資料外洩或遺失等情形，必須廢止憑證時，憑證用戶應於事件發生後一個工作天內通知本憑證中心之註冊窗口；註冊中心操作員則於憑證用戶之身分驗證審核通過後，一個工作天內完成憑證廢止作業。憑證用戶仍應承擔本憑證中心實際完成憑證廢止或暫停前所有使用該憑證的法律責任。

6、其他重要事項

- (1)如因本憑證中心之系統維護、轉換及擴充等需要，得暫停部分憑證服務，並公告及通知憑證用戶；憑證用戶或信賴憑證者不得以此作為要求本憑證中心損害賠償的理由。
- (2)憑證用戶在接受本憑證中心所簽發之憑證後，即表示已確認憑證內容資訊之正確性，並依照本作業基準相關規定使用憑證；如憑證內容資訊有誤，憑證用戶應主動通知註冊窗口重新確認，並由註冊窗口以公文書或電子表單方式通知註冊中心操作員於一個工作天內簽發新憑證。

- (3)憑證用戶及信賴憑證者應慎選安全的電腦環境及可信賴的應用系統，如因電腦環境或應用系統本身因素，導致憑證用戶權益受損時，應自行承擔責任。
- (4)信賴憑證者接受使用本憑證中心簽發的憑證時，即表示已了解並同意有關本憑證中心法律責任之條款，並依照本作業基準相關規定使用憑證。

1 簡 介

1.1 概 述

本院為提供憑證用戶於使用本院認可之資訊交易平台時，所需要的身分認證、加密及簽章，乃建置本憑證中心，進而提供認證等相關服務。本院負責本作業基準之訂定及修訂，本作業基準由本院依電子簽章法相關規定，經該法主管機關經濟部核定後公布。本院並未授權本憑證中心以外的憑證機構簽發憑證。

1.2 文件與識別

1.2.1 文 件

本作業基準之名稱為立法院憑證管理中心憑證實務作業基準(The Legislative Yuan Certification Authority Certification Practice Statement)版本為第 1.2 版，依循憑證政策與 RFC 3647 格式製作。最新版本的本作業基準與憑證政策，可在本憑證中心網站 (<http://ca.ly.gov.tw>)取得。

1.2.2 識 別

本憑證中心之物件識別碼(Object Identifier, OID)為 2.16.886.101.20004.1。

1.3 公開金鑰基礎建設參與成員

1.3.1 憑證中心

依據憑證政策的規定，本憑證中心是本院公開金鑰基礎建設(Public Key Infrastructure, PKI，以下簡稱本基礎建設)的第一層憑證機構，並遵照本作業基準，除負責本憑證中心之自簽憑證外，同時負責本院之立法委員憑證、公費助理憑證、職員憑證、伺服器應用憑證、外包廠商憑證、外單位憑證、院內單位臨時憑證與傳播媒體憑證等憑證之簽發及管理作業。

1.3.2 註冊中心

- (1) 註冊中心設置註冊中心伺服器(RA Server)，註冊中心伺服器由註冊中心操作員(RA Operator, RAO)負責管理，註冊中心操作員直接歸屬本院資訊處。
- (2) 註冊中心授權由本院資訊處、人事處、總務處與秘書處做為註冊窗口(RA Counter)，並依照第 1.3.5(1)章節規定辦理憑證用戶之身分識別與相關文件審核作業，最後由註冊中心操作員經由網路連線至本憑證中心，進行後續處理。
- (3) 註冊中心操作員負責產製憑證用戶的金鑰對或接受憑證用戶自行產製的金鑰對，同時送交憑證申請或廢止之請求至本憑證中心，申辦成功後將資料與用戶之憑證寫入 IC 卡或其他載具內。

1.3.3 憑證用戶

憑證用戶係指記載於本憑證中心所簽發憑證的憑證主體名稱(Certificate Subject Name)的個體，包括本院委員、公費助理、職工同仁、聘僱人員、以及特殊專案申請者(包

含資訊外包廠商、媒體記者、本院卸任委員、退休職工人員或其他特殊使用者等)。

1.3.4 信賴憑證者

- (1) 信賴憑證者係指相信本憑證中心所簽發憑證之憑證主體名稱與公開金鑰之連結關係的個體。
- (2) 信賴憑證者在使用本憑證中心所簽發之憑證前，必須以本憑證中心自簽憑證及憑證狀態資訊，檢驗所使用憑證的有效性。在確認憑證的有效性後，才可使用憑證進行以下作業：
 - a. 檢驗電子文件的數位簽章之正確性。
 - b. 檢驗電子文件簽章者之身分。

1.3.5 其他參與成員

- (1) 註冊窗口
 - a. 註冊中心授權於本院資訊處、人事處、總務處與秘書處設立註冊窗口，或經由本憑證中心授權核可的單位來擔任，其設置的地點需在該單位內。
 - b. 註冊窗口之主要任務是負責受理憑證用戶之憑證註冊申請、暫停使用申請、恢復使用申請及廢止申請等業務。
 - c. 註冊窗口依作業規定對憑證用戶進行身分識別與相關文件審核作業，並於確認身分後，以公文書或電子表單方式函送本院資訊處。
- (2) 儲存庫
 - a. 本憑證中心自行建置及維運儲存庫，儲存庫為符合 X.500 標準的目錄伺服器，負責公告本憑證中心自簽憑證、所簽發之憑證、憑證廢止清冊(Certificate Revocation List, CRL)及其他憑證相關資訊。
 - b. 本憑證中心發行之憑證與憑證廢止狀態，可由憑證管理系統同步更新於儲存庫中，提供憑證用戶查詢最新的資訊。
 - c. 儲存庫提供全天 24 小時之服務。
- (3) 本憑證中心網站
 - a. 本憑證中心建置專屬網站，負責公告本作業基準與憑證政策。
 - b. 提供憑證用戶下載本憑證中心自簽憑證與憑證廢止清冊。
 - c. 提供憑證用戶以員工編號、中文姓名或電子郵件信箱查詢經憑證用戶同意對外公開之相關憑證。
 - d. 本憑證中心網站提供本院憑證用戶，全天 24 小時之服務，其網址為：
<http://ca.ly.gov.tw/>。

1.4 憑證適用性

1.4.1 適用範圍

適用於本憑證中心認可之資訊交易平台應用所需之身分認證、加密與簽章，範圍如下：

- (1) 本院應用系統之身分認證。
- (2) 本院與其他政府機關之電子資料交換。
- (3) 本院相關電子公文、表單、檔案與郵件之加密與簽章。
- (4) 本院應用系統網站的安全傳輸服務。

1.4.2 限制範圍

- (1) 憑證用戶在使用私密金鑰時，應慎選安全的電腦環境及可信賴的應用系統，以避免私密金鑰被惡意軟硬體盜取或誤用而引發權益受損。
- (2) 憑證用戶在使用本憑證中心所提供之認證服務前，必須了解及同意本作業基準與使用的業務系統等相關作業之規範、權利與義務，且僅於憑證使用目的範圍內信賴該憑證，及無任何違反法律與侵害第三者的權利，同時必須注意本作業基準之修訂。

1.5 政策管理

1.5.1 管理單位

本憑證中心負責維護本作業基準，經電子簽章法主管機關依據相關規定核定後，於本憑證中心網站(<http://ca.ly.gov.tw>)公布施行。

1.5.2 聯絡窗口

對於本作業基準之任何疑問或建議，以及憑證用戶有關憑證的註冊、申請、更新、查詢與金鑰有遺失或不安全顧慮的疑議時，請以下列方式聯絡：

- (1) 聯絡電話：02-23585858 分機 1714
- (2) 郵遞地址：台北市中正區中山南路一號(立法院資訊處)
- (3) 電子郵件信箱：ca@ly.gov.tw

1.5.3 憑證實務作業基準之審定

本憑證中心應先自行檢查本作業基準，是否符合憑證政策相關規定後，本憑證中心便可正式引用本基礎建設的憑證政策。另依據我國電子簽章法規定，本作業基準必須經主管機關經濟部核定。

1.5.4 憑證實務作業基準審定程序

- (1) 本作業基準經電子簽章法主管機關核定後，由本憑證中心公布。
- (2) 本作業基準修訂後經主管機關審核生效，除另有規定外，如修訂之內容與本作業

基準有所牴觸時，以修訂之內容為準。

- (3) 如以附加文件方式修訂，而該附加文件之內容與本作業基準有所牴觸時，以該附加文件之內容為準。

1.6 本文件相關定義與縮寫

CA (Certificate Authority，憑證管理中心)

CP (Certificate Policy，憑證政策)

CPS (Certification Practice Statement，憑證實務作業基準)

CRL (Certificate Revocation List，憑證廢止清冊)

DN (Distinguished Name，唯一識別名稱)

OCSP (Online Certificate Status Protocol，線上憑證狀態協定)

OID (Object IDentifiers，物件識別碼)

RA (Registration Authority，註冊中心)

RAO (RA Operator，註冊中心操作員)

2 一般條款

2.1 職責及義務

2.1.1 立法院之職責

本院提供一安全訊息的基礎建設，使憑證及公鑰加密得以安全運作。本憑證中心在此基礎建設中為信任的最高點，其階層架構下包含一個註冊中心。

2.1.2 憑證中心之職責

- (1) 依據本作業基準運作。
- (2) 產製其自身與註冊中心的金鑰，並簽署其自身與註冊中心的憑證及公告其公開金鑰。
- (3) 簽發、公布及廢止憑證。
- (4) 簽發及公布憑證廢止清冊。
- (5) 執行本憑證中心相關人員之識別及鑑別程序。
- (6) 告知註冊中心、註冊窗口，有關本憑證中心及註冊中心之義務與責任。

2.1.3 註冊中心之職責

- (1) 依據本作業基準運作。
- (2) 將憑證用戶之申請資料及公開金鑰，透過安全管道傳送至本憑證中心。
- (3) 執行註冊中心操作員之識別及鑑別程序。
- (4) 告知註冊窗口有關註冊窗口之義務與責任。
- (5) 告知憑證用戶及信賴憑證者，有關本憑證中心及註冊中心之義務與責任。
- (6) 告知憑證用戶及信賴憑證者，有關接受或使用本憑證中心所簽發之憑證，必須遵守本作業基準之相關規定。

2.1.4 憑證用戶之義務

- (1) 詳閱本作業基準，並應遵守其中所列之相關規定。
- (2) 提供完整及正確的個人資料給註冊窗口來鑑別身分。
- (3) 填寫及簽署「立法院數位憑證暨 IC 識別證申請表」(以下簡稱申請表)。
- (4) 憑證用戶必須確實且妥善安全地保護其私密金鑰。
- (5) 憑證用戶必須依本作業基準摘要之第 2、3、4、5、6 項規定，合法且正確地使用私密金鑰與憑證。
- (6) 憑證用戶端的私密金鑰有被冒用、曝露或遺失等不安全的顧慮時，憑證用戶必須依照第 4.9 章節規定，向本憑證中心或註冊窗口辦理憑證廢止申告。

2.1.5 信賴憑證者之義務

- (1) 信賴憑證者使用或接受他人(本憑證中心或憑證用戶)的憑證前，應依據本作業基準及憑證內容所規定的業務範圍，確認該憑證的合法用途，並於該憑證使用目的範圍內信賴該憑證。
- (2) 使用本憑證中心簽發憑證之相關業務系統，不應違反相關法律的規定與侵害第三者的權利。
- (3) 信賴憑證者使用或接受他人的憑證時，應依據本作業基準、應用業務系統作業規範的規定及 X.509 憑證標準的規範，由憑證鏈逐一驗證該憑證的正確性及有效性。
- (4) 信賴憑證者使用或接受他人的憑證時，應從憑證廢止清冊或利用線上憑證狀態查詢方式檢查憑證的狀態，確認憑證是否為廢止或暫時停用。

2.1.6 儲存庫服務之義務

儲存庫定期公布本憑證中心所簽發之憑證、憑證廢止清冊及其它憑證相關資訊。

2.2 法律責任

2.2.1 憑證中心之責任

- (1) 保證範圍及其限制條件：本憑證中心依憑證政策進行運作，並遵守本作業基準規定之程序，簽發及管理憑證、簽發並公布憑證廢止清冊及維持儲存庫正常運作。
- (2) 否認聲明及其限制條件：憑證用戶或信賴憑證者如未依照第 1.4.1 章節規定之適用範圍使用憑證所引發之後果，本憑證中心不負任何法律責任。
- (3) 其他除外條款：
 - a. 如因不可抗力或其他非可歸責於本憑證中心之事由，所導致之損害事件，本憑證中心不負任何法律責任。
 - b. 如因本憑證中心之系統維護、轉換及擴充等需要，得暫停部分憑證服務，並公告於本憑證中心網站，憑證用戶或信賴憑證者不得以此作為要求本憑證中心損害賠償之理由。
 - c. 如因第 4.9.1 章節廢止憑證之事由，憑證用戶應依照第 4.9.3 章節憑證廢止程序向本憑證中心提出廢止憑證申請，本憑證中心會在一個工作天內核定廢止憑證申請，並完成憑證廢止作業、簽發憑證廢止清冊及公告於儲存庫與本憑證中心網站。憑證用戶於憑證廢止狀態未被公布之前，應採取適當的行動，以減少對信賴憑證者之影響，並承擔所有因使用該憑證所引發之責任。

2.2.2 註冊中心之責任

- (1) 保證範圍及其限制條件
 - a. 註冊中心遵守本作業基準規定之程序，負責收集和驗證憑證用戶的身分及憑

證相關資訊之註冊工作，註冊中心因執行註冊工作所引發之法律責任，除法令另有規定外，由本憑證中心負責。

- b. 本憑證中心所簽發之憑證僅對憑證主體身分做確認，由註冊中心操作員審驗憑證用戶之身分及憑證相關資訊；如因憑證用戶隱瞞事實，提供註冊窗口不正確資料，導致信賴憑證者遭受損害時，如該損害之造成不可歸責於註冊窗口時，應由憑證用戶自負損害賠償之責。
- (2) 否認聲明及其限制條件：憑證用戶或信賴憑證者應依照第 1.4.1 章節規定之適用範圍使用憑證。
 - (3) 其他除外條款：如因不可抗力或其他非可歸責於註冊中心之事由，所導致之損害事件，註冊中心不負任何法律責任。

2.3 財務責任

2.3.1 憑證中心之賠償責任

本憑證中心之賠償責任依據下列規定辦理：

- (1) 本憑證中心處理憑證用戶的註冊資料及憑證簽發作業，除未遵照本作業基準及相關作業的規定辦理，而造成憑證用戶的損失，且可歸責於本憑證中心的過失外，本憑證中心概不負任何損害賠償責任。
- (2) 如因網際網路傳輸中斷、設備故障或其他不可抗拒的天災事故(戰爭或地震等)，而非本憑證中心作業人員故意或過失，致所簽發的憑證造成憑證用戶損失時，本憑證中心概不負任何損害賠償責任。
- (3) 本憑證中心如因作業人員故意或過失，未遵照本作業基準與相關作業規定辦理憑證註冊、簽發與廢止作業，而造成憑證用戶的損失，作業人員依公務人員服務相關規定辦理。
- (4) 憑證用戶或其他有權者提出憑證廢止或暫停的要求後，至本憑證中心實際完成廢止或暫停該憑證為止的期間內，若該憑證用戶的憑證被用以進行非法交易，或進行交易後產生法律糾紛時，本憑證中心依據本作業基準與相關作業規範執行處理作業時，則不負任何損害賠償責任。
- (5) 憑證用戶或信賴憑證者透過本憑證中心，查詢所簽發憑證的憑證狀態時，若非因本憑證中心之作業緣故，致傳遞予憑證用戶或信賴憑證者的資訊錯誤，而導致憑證用戶或信賴憑證者損失時，本憑證中心不負任何賠償責任。

2.3.2 註冊中心之賠償責任

註冊窗口必須善盡保管憑證用戶的註冊與相關資料的責任，避免洩漏、冒用、篡改或任意使用相關資訊，註冊窗口或註冊中心操作員因處理憑證註冊，發生錯誤而造成憑證用戶或信賴憑證者損害時，其作業人員應依公務人員服務相關規定辦理。

2.3.3 憑證用戶之賠償責任

- (1) 損害賠償責任：憑證用戶向註冊窗口申請註冊時，因故意、過失或不正當意圖而提供不實資料，致造成註冊中心、憑證中心或信賴憑證者遭受損害時，應由該憑證用戶負一切損害賠償責任。
- (2) 妥善保管其私密金鑰與密碼：憑證用戶應妥善保管其私密金鑰與密碼，不得洩漏或交付予他人使用，如因故意或過失，致造成註冊中心、憑證中心或信賴憑證者遭受損害時，應由該憑證用戶負一切損害賠償責任。
- (3) 違反本作業基準及相關作業規範：憑證用戶申請使用憑證，有違反本作業基準及相關作業規範，或憑證使用於非本作業基準規定的其他業務範圍，致造成註冊中心、憑證中心或信賴憑證者遭受損害時，應由該憑證用戶負一切損害賠償責任。

2.3.4 對憑證用戶及信賴憑證者之賠償責任

憑證用戶或信賴憑證者因使用憑證而發生損害賠償事件時，本憑證中心之損害賠償責任依照本作業基準摘要之第 4、5 項及第 1.4、2.3.1、2.3.2、2.8.3 章節規定辦理。

2.3.5 財務保險與財會稽核

本憑證中心營運所需之經費由本院每年依所編列政府預算提撥，未向保險公司投保，但本院每年均由審計部執行財會稽核。

2.4 解釋及施行

2.4.1 政府法令

本作業基準受中華民國法律所管轄與督導，接受主管機關相關法律規範。

2.4.2 適用性

本作業基準的條文有不適用而必須修正時，其他條文仍屬有效，該項不適用條文的更新，依本作業基準的規定辦理。

2.4.3 仲 裁

憑證用戶與本憑證中心遇有爭議時，雙方應本誠信原則協商解決。如協商不成須訴訟時，雙方同意以臺北地方法院為第一審管轄法院。

2.5 費 用

2.5.1 憑證申請及更新費用

本憑證中心對向本院提出憑證申請及更新的憑證用戶，暫不收取任何費用。

2.5.2 憑證查詢費用

本憑證中心暫不收取任何憑證查詢費用。

2.5.3 憑證廢止及狀態查詢費用

本憑證中心對憑證用戶及憑證信賴者，進行的憑證廢止及狀態查詢，暫不收取任何費用。

2.5.4 退 費

本憑證中心目前沒有收費，因此無請求退費之程序。

2.6 公布與儲存庫

2.6.1 儲存庫

除系統維護的需求外，本憑證中心提供簽發之憑證、憑證廢止清冊及其他憑證相關資訊之即時性查詢服務。

2.6.2 憑證中心之資訊公布

本憑證中心之相關資訊公布於網站上(<http://ca.ly.gov.tw>)：

- (1) 本憑證中心相關最新訊息。
- (2) 本作業基準。
- (3) 憑證政策。
- (4) 憑證廢止清冊下載。
- (5) 本憑證中心自簽憑證下載。
- (6) 憑證查詢。
- (7) 本憑證中心對於憑證用戶資訊的保護，皆依照行政院公告之「個人資料保護法」的規範運作，及其他政府單位相關的規範運作。

2.6.3 公布頻率

- (1) 新版憑證政策經核定生效後，以及經修改完成之新版憑證實務作業基準，均於主管機關核准後，即公告於本憑證中心網站。
- (2) 本憑證中心所簽發之憑證廢止清冊，於簽發後即時公布於儲存庫。
- (3) 本憑證中心自簽憑證，於簽發後即時公布於儲存庫。
- (4) 簽發之憑證，於簽發後即時公布於儲存庫。
- (5) 本憑證中心所簽發之憑證廢止清冊，每天一次更新於本憑證中心網站。

2.6.4 存取控制

- (1) 本憑證中心之主機建置於防火牆內部，除本憑證中心授權的註冊中心伺服器外，不允許外界直接連線到本憑證中心之主機。
- (2) 儲存於儲存庫中的憑證與憑證廢止資訊，僅開放憑證用戶透過介面查詢使用，但不提供修改的功能，憑證用戶必須依照本憑證中心儲存庫的安全管控措施執行存取。

2.7 稽 核

2.7.1 稽核的頻率

本憑證中心接受每年一次的外部稽核與兩次的內部稽核，以確認相關運作符合本作

業基準所定的安全規定與程序。

2.7.2 稽核者身分鑑別及資格

執行稽核作業的稽核人員，至少須對本基礎建設有相關稽核經驗，且熟悉本作業基準的運作規範，及具備應用系統的業務執行與電腦硬軟體相關知識，甚至具有系統規劃及設計開發等相關經驗。

2.7.3 被稽核單位與稽核者關係

- (1) 本憑證中心的稽核人員與被稽核單位，必須無任何業務往來或利害關係，並以獨立、公正、客觀的態度執行查核評估。
- (2) 當適任的稽核人力不足時，可以委由專業且公正、客觀的專業稽核公司，代為執行稽核相關作業。

2.7.4 稽核範圍

- (1) 本憑證中心是否遵照本作業基準運作。
- (2) 註冊中心與註冊中心操作員是否遵照本作業基準及註冊中心作業規範運作。
- (3) 註冊窗口是否遵照本作業基準及註冊中心作業規範運作。
- (4) 稽核人員主要稽核項目包括業務執行的公告、服務的完整性、本憑證中心環境的安全控管。

2.7.5 對於稽核結果之因應方式

稽核報告應提交給被稽核單位，當發現稽核缺失行為，被稽核單位應適當的採取矯正措施並追蹤改善後的情形。

2.7.6 稽核結果查詢

稽核結果包含敏感的機密資訊，只有受檢單位與相關稽核人員可知悉，非經受檢單位的授權稽核單位，絕不洩露予其他人員取得或知悉。

2.8 機密及隱私

2.8.1 機密資訊種類

- (1) 註冊資訊：本院所蒐集及擁有的資訊，只能使用在本基礎建設之運作上，或是相關的資料傳輸上，註冊紀錄視為機密文件，本作業基準所支援的個人資訊搜集將可歸類成以下：
 - a. 註冊窗口所取得的個人資料：做為身分鑑別。
 - b. 憑證中心所取得的個人資料：做為憑證資訊。
- (2) 憑證資訊：註冊中心產生憑證註冊紀錄時，同時會取得一些相關資訊，所蒐集的資訊將會出現在 X.509 v.3 憑證上。憑證上所載入的資訊是註冊紀錄的一部份，不具機密性，而註冊紀錄的其他資訊則是具機密的，憑證用戶的註冊基本資料與身分認證資料，非經由憑證用戶同意或符合法令規定，絕不任意對外公開。

2.8.2 非機密資訊的種類

- (1) 憑證資訊：公告在儲存庫上的憑證資訊、憑證狀態(提供憑證有效性狀態查詢功能時)、及本憑證中心網站上的公開憑證資訊、憑證政策與本作業基準，均為可公開的非隱密性資訊。
- (2) 公開憑證廢止的資訊：本憑證中心定期將憑證廢止資訊，公告在儲存庫上。憑證廢止資訊包含在憑證廢止清冊中，透過儲存庫進行公告作業，廢止決定的資訊仍舊是屬機密資料，僅有廢止的事實可透過儲存庫來公告。

2.8.3 隱私權保護

本憑證中心依照個人資料保護法，蒐集、處理及利用憑證用戶的認證申請資料。

2.9 智慧財產權

2.9.1 一般條款

本院保證本作業基準所使用的軟硬體，均屬於本院財產，並具有合法的使用權力。本院拒絕接納任何違反智慧財產權的傾向及行為。

- (1) 本基礎建設：除非本院授權，本基礎建設中之任何文件、圖形、計畫的智慧財產權歸屬於本院，本作業基準不歸屬於任何第三者。
- (2) 公鑰與私鑰：除非有任何其他合約規定，在本憑證中心階層架構下所產製的任何公鑰與私鑰，其智慧財產歸屬於本院。當憑證用戶的金鑰有洩漏之虞，本院保留廢止金鑰與憑證的權力。
- (3) 憑證：除非有任何其他合約規定，在本憑證中心階層架構下所簽發的任何憑證，其智慧財產歸屬於本院。本院同意在本憑證中心下所簽發的憑證，憑證用戶可以免費使用，一但憑證可能洩漏時，本院保留廢止金鑰與憑證的權力。
- (4) 識別名稱：除非有其他規定，識別名稱的智慧財產權，應由註冊中心來指定。

2.9.2 著作權

本作業基準的智慧財產屬於本院擁有，可由本憑證中心網站自由下載，或依著作權法相關規定重製或散布，必須保證是完整複製，並註明著作權為本院所擁有。另外，重製或散布本作業基準者，不得向他人收取費用，亦不得拒絕任何人請求取得。本院對於不當使用或散布本作業基準所引發之一切結果，不負任何法律責任。

3 識別及鑑別

3.1 命名

3.1.1 命名種類

本憑證中心所簽發憑證之憑證主體名稱，採用 X.500 唯一識別名稱(Distinguished Name, DN)。

3.1.2 命名須有意義

組織及個人之憑證主體名稱，必須符合我國相關法令對該主體命名之規定，並且使用正式登記的名稱；設備與伺服器應用軟體之憑證主體名稱，必須為該設備與伺服器應用軟體之管理者的名稱或經國際認證合法網路主體名稱，同時其中的通用名稱(Common Name, CN)應以易於瞭解為原則(中文名稱、模組名稱、序號或應用程序等)。

3.1.3 憑證用戶之匿名與假名

本憑證中心不允許憑證用戶使用匿名與假名。

3.1.4 命名形式之解釋規則

命名形式之解釋規則由本院負責建立，並包含在憑證格式剖繪中。

3.1.5 命名之獨特性

本憑證中心的 X.500 唯一識別名稱為：C=TW，O=The Legislative Yuan，OU=CA，CN = The Legislative Yuan CA。

為使本憑證中心所簽發憑證的憑證主體名稱具備獨特性，本憑證中心採用以下名稱格式：

- (1) 立法委員憑證：C=TW，O=The Legislative Yuan，OU=The Legislator，OU=委員
屆別，OU=委員卡號，Employee Number=員工編號，DN_UID=員工編號，Surname=
中文姓名，CN=中文姓名，Mail=電子信箱，Employee Type=卡別，UPN=電子信箱。
- (2) 公費助理憑證：C=TW，O=The Legislative Yuan，OU=Assistant，Employee Number=
助理編號，OU=助理屆別，DN_UID=助理編號，Surname=中文姓名，CN=中文
姓名，Mail=電子信箱，Employee Type=卡別，UPN=電子信箱。
- (3) 職員憑證：C=TW，O=The Legislative Yuan，OU=Employee，Department Number=
處科別代碼，Employee Number=員工編號，DN_UID=員工編號，Surname=中文
姓名，CN=中文姓名，Mail=電子信箱，Employee Type=卡別，UPN=電子信箱。
- (4) 伺服器應用憑證：C=TW，O=The Legislative Yuan，OU=Server，OU=承辦單位
代碼，Surname=系統名稱，CN=識別名稱。
- (5) 外包廠商憑證：C=TW，O=The Legislative Yuan，OU=Vender，OU=承辦單位代
碼，Employee Number=帳號，DN_UID=帳號，Surname=中文姓名，CN=公司名
稱，Mail=電子信箱，Employee Type=卡別，UPN=電子信箱。
- (6) 外單位憑證：C=TW，O=The Legislative Yuan，OU=Guest，OU=承辦單位代

碼，Employee Number=帳號，DN_UID=帳號，Surname=中文姓名，CN=單位名稱，Mail=電子信箱，Employee Type=卡別。

- (7) 院內單位臨時憑證：C=TW，O=The Legislative Yuan，OU=Temporary，OU=承辦單位代碼，Employee Number=帳號，DN_UID=帳號，Surname=中文姓名，CN=單位名稱，Mail=電子信箱，Employee Type=卡別。
- (8) 傳播媒體憑證：C=TW，O=The Legislative Yuan，OU=Reporter，OU=承辦單位代碼，Employee Number=帳號，DN_UID=帳號，Surname=中文姓名，CN=單位名稱，Mail=電子信箱，Employee Type=卡別，UPN=電子信箱。

3.1.6 商標之辨識、鑑別及角色

當憑證主體名稱可能包含商標時，則其命名必須符合我國商標相關法規。

3.2 初始驗證

3.2.1 證明擁有私密金鑰之方式

- (1) 如憑證由註冊中心操作員代為產製金鑰對，簽發憑證時由註冊中心透過數位信封及數位簽章方式，將憑證用戶之公開金鑰傳送至本憑證中心，因此憑證用戶在申請憑證時不必證明持有私密金鑰。
- (2) 如憑證用戶自行產製金鑰對，則必須使用金鑰對產生憑證申請檔，再將憑證申請檔交給註冊中心，註冊中心將使用該用戶的公開金鑰驗證該憑證申請檔的簽章，以證明憑證用戶擁有相對應的私密金鑰。

3.2.2 個人身分鑑別之程序

本院個人身分鑑別主要以本院立法委員、公費助理、職員與技工工友、本院卸任委員、退休職工人員或其他特殊使用者為對象，相關申辦人之鑑別程序如下：

- (1) 個人申請之身分鑑別程序：申請者依據本院人事單位之權責，由本人指派他人或親自至本院相關負責的註冊窗口辦理憑證申請，並由本院註冊窗口驗證申請人之身分資料，以確認為本人，並核對申請表之個人資料，包括姓名、身分證字號、申請人單位、員工編號等。
- (2) 線上申請之身分鑑別程序：申請者以電子表單申請方式，向本院註冊窗口提出申請，身分鑑別工作由表單系統與註冊窗口負責申請者之身分認證。
- (3) 集體申請之身分鑑別程序：申請者以集體申請方式，向本院註冊窗口提出申請，身分鑑別工作由本院註冊窗口負責執行。

3.2.3 組織身分鑑別之程序

- (1) 政府機關(構)、單位之身分鑑別程序：政府機關(構)或本院內部單位，必須將申請表以公文書方式進行申請，註冊窗口將驗證公文書之完整性及申請表內容之正確性。
- (2) 公司行號、媒體之身分鑑別程序：外包廠商或媒體業者，除必須將申請表以公文書方式進行申請外，並應提供主管機關或合法授權單位核發的相關證明文件(影

本必須加蓋公司章與負責人章)，或外國公司合法的相關證明文件，如為公司授權代理人辦理，需授權代理人親自辦理，且驗證該授權代理人的相關身分證明文件；媒體業者則須向本院秘書處提出申請，身分鑑別工作由本院秘書處負責執行。

3.2.4 硬體裝置或伺服器軟體鑑別之程序

政府機關(構)或本院內部單位，必須以系統管理者身分提出憑證申請，將申請表以公文書或電子表單方式函送註冊窗口，註冊窗口將驗證公文書之完整性與申請表內容之正確性。

3.3 金鑰更換

3.3.1 憑證之金鑰更換

憑證之金鑰更換係指簽發一張與舊憑證具有相同特徵的新憑證，而新的憑證除有新的、不同的公開金鑰(對應新的、不同的私密金鑰)及不同的序號外，不同的憑證亦可能被指定不同的有效期限。

(1) 本憑證中心在以下兩種情形會更換金鑰，並簽發新的自簽憑證：

- a. 目前使用之金鑰生命週期結束。
- b. 目前使用之金鑰的安全性有問題時(懷疑或確定金鑰被破解)。

(2) 本憑證中心簽發之憑證效期，主要依據憑證類別的不同，而具有不同的憑證效期，如憑證用戶之私密金鑰使用期限屆滿必須更換金鑰時，應向本憑證中心重新申請憑證，註冊中心將依照第 3 章節規定，對於重新申請憑證之憑證用戶進行識別及鑑別。

3.3.2 廢止憑證之金鑰更換

如憑證用戶的私密金鑰，因憑證廢止而必須更換金鑰時，應向本憑證中心重新申請憑證，註冊窗口將依相關規定，對於重新申請憑證之憑證用戶進行識別及鑑別。

3.4 憑證廢止之識別與鑑別程序

本憑證中心之憑證廢止作業程序依第 4.9.3 章節規定進行。憑證廢止申請時之身分鑑別需指派他人或臨櫃填寫申請表，註冊窗口審核確認為真正憑證用戶或授權代理人之廢止申請後，本憑證中心始進行憑證廢止作業。

4 營運規範

4.1 憑證申請

4.1.1 申請者

憑證用戶指派他人或親自擔任申辦人，代表該憑證用戶申請憑證。

4.1.2 申請登記過程

憑證申辦人應閱讀憑證政策，如同意政策內容，則填寫申請表。

4.2 申請憑證之程序

4.2.1 立法委員憑證

- (1) 新任委員到任時，得由本院人事處統一彙整資料代為申請，或由委員授權他人或親自擔任臨櫃申辦人，代表該憑證用戶填寫申請表。
- (2) 本院人事處的註冊窗口負責驗證委員之身分，並確認所提供之彙整資料或填寫之申請表的資料內容無誤，最後將審核完成的彙整資料或申請表，以公文書或電子表單方式函送本院資訊處。
- (3) 最後由註冊中心操作員代為產製金鑰對及註冊憑證。

4.2.2 公費助理憑證

- (1) 公費助理得由委員或黨團同意後，由本人授權他人或親自擔任臨櫃申辦人，代表該憑證用戶填寫申請表。
- (2) 本院人事處的註冊窗口負責驗證公費助理之身分，並確認所填寫之申請表的資料內容無誤，最後將審核完成的申請表，以公文書或電子表單方式函送本院資訊處。
- (3) 最後由註冊中心操作員代為產製金鑰對及註冊憑證。

4.2.3 職員憑證

- (1) 本院職工人員於報到時，由本人授權他人或親自擔任臨櫃申辦人，代表該憑證用戶填寫申請表。
- (2) 本院人事處與總務處的註冊窗口，分別負責一般職員及技工工友之身分驗證，並確認所填寫之申請表的資料內容無誤，最後將審核完成的申請表，以公文書或電子表單方式函送本院資訊處。
- (3) 最後由註冊中心操作員代為產製金鑰對及註冊憑證。

4.2.4 伺服器應用憑證

- (1) 政府機關(構)或本院內部單位，必須以系統管理者身分提出憑證申請，代表該憑證用戶填寫申請表。
- (2) 如伺服器為自行產製私密金鑰與憑證資料，則系統管理者須將憑證申請檔連同申請表，以公文書或電子表單方式函送本院資訊處的註冊窗口。
- (3) 註冊窗口負責驗證公文書之完整性與申請表內容之正確性。

- (4) 最後由註冊窗口依據申請資料，決定是否代為產製金鑰對及註冊憑證。

4.2.5 外包廠商憑證

- (1) 外包廠商必須提供主管機關或合法授權單位核發的相關證明文件(影本必須加蓋公司章與負責人章)，或外國公司合法的相關證明文件，代表該憑證用戶填寫申請表，並以公文書方式函送本院資訊處的註冊窗口。
- (2) 註冊窗口負責驗證公文書之完整性與申請表內容之正確性。
- (3) 最後由註冊中心操作員代為產製金鑰對及註冊憑證。

4.2.6 外單位憑證

- (1) 外單位(含本院卸任委員、退休職工人員或其他特殊使用者)必須授權他人或親自擔任臨櫃申辦人，代表該憑證用戶填寫申請表，並以公文書方式分別函送本院相關負責的註冊窗口。
- (2) 註冊窗口負責驗證公文書之完整性與申請表內容之正確性。
- (3) 最後由註冊中心操作員代為產製金鑰對及註冊憑證。

4.2.7 院內單位臨時憑證

- (1) 本院內部單位如需申請臨時憑證，必須由該單位授權代理人擔任臨櫃申辦人，代表該憑證用戶填寫申請表，並以公文書方式函送本院資訊處的註冊窗口。
- (2) 註冊窗口負責驗證公文書之完整性與申請表內容之正確性。
- (3) 最後由註冊中心操作員代為產製金鑰對及註冊憑證。

4.2.8 傳播媒體憑證

- (1) 媒體單位如需申請本院之憑證，必須提供主管機關或合法授權單位核發的相關證明文件(影本必須加蓋公司章與負責人章)，或外國公司合法的相關證明文件，代表該憑證用戶填寫申請表，並以公文書方式函送本院秘書處的註冊窗口。
- (2) 註冊窗口負責驗證公文書之完整性與申請表內容之正確性，並將審核完成的申請表，以公文書或電子表單方式函送本院資訊處。
- (3) 最後由註冊中心操作員代為產製金鑰對及註冊憑證。

4.3 簽發憑證之程序

註冊窗口於收到憑證申請資料後，將依照第 3.2 章節規定，進行申辦人身份鑑別程序，以作為判定是否同意簽發憑證之依據。

4.3.1 憑證中心簽發憑證

- (1) 憑證用戶首先必須將相關申請資料，以公文書或電子表單方式函送註冊窗口，所有憑證用戶在憑證註冊時，必須驗證身分來符合本作業基準的規定。
- (2) 當憑證用戶於憑證註冊程序進行時，由憑證用戶自行提供或註冊中心操作員端產

製用戶金鑰，同時將申請表中屬於憑證資訊的部分資料輸入上傳至註冊中心。

- (3) 註冊中心將個人資訊與公鑰，傳送本憑證中心審核及簽發憑證，同時將憑證資料傳送給憑證用戶，憑證用戶亦可連線至儲存庫或本憑證中心網站下載憑證。
- (4) 本憑證中心回傳所簽發之憑證，並由註冊中心操作員寫入憑證用戶之憑證載具中。

4.3.2 憑證中心明確告知申請者

本憑證中心或註冊中心如不同意簽發憑證，將以適當方式通知憑證申請者，並明確告知不同意簽發的理由，除因申請者之身分識別與鑑別的原因外，本憑證中心得因其他原因不同意簽發憑證。

4.4 接受憑證之程序

4.4.1 接受憑證程序

憑證用戶在收到憑證時，應檢查憑證相關資訊是否正確，如發現任何錯誤，應於一個工作天內通知註冊窗口處理。

4.4.2 憑證中心公布此憑證

本憑證中心在簽發憑證後，自動將簽發之憑證公布到儲存庫上。

4.5 金鑰對和憑證使用

4.5.1 用戶私鑰和憑證使用

- (1) 憑證用戶係指記載於本憑證中心所簽發憑證的憑證主體名稱的個體，包括組織與代表組織行使業務之個人。
- (2) 憑證用戶必須依照第 3 章節之識別及鑑別程序，進行憑證申請作業。
- (3) 憑證用戶之 IC 卡遺失或憑證過期後，必須依照第 3 章節之識別及鑑別程序，重新辦理憑證申請。

4.5.2 可信賴用戶公鑰和憑證使用

- (1) 信賴憑證者係指相信本憑證中心所簽發憑證之憑證主體名稱與公開金鑰之連結關係的個體。
- (2) 信賴憑證者在使用本憑證中心所簽發之憑證前，必須以本憑證中心自簽憑證及憑證狀態資訊，檢驗所使用憑證的有效性，在確認憑證的有效性後，才可使用憑證進行以下作業：
 - a. 檢驗電子文件的數位簽章之正確性。
 - b. 檢驗電子文件簽章者之身分。

4.6 憑證更新

4.6.1 憑證更新事由

本憑證中心不接受憑證更新，如憑證到期時，必須重新申請與舊憑證相同屬性的新憑證，重新申請時請參考第 4.1、4.2、4.3 及 4.4 章節規定。

4.6.2 憑證更新申請者

請參考第 4.6.1 章節規定。

4.6.3 憑證更新請求

請參考第 4.6.1 章節規定。

4.6.4 公告憑證更新給憑證用戶

請參考第 4.6.1 章節規定。

4.6.5 已更新憑證的接受程序

請參考第 4.6.1 章節規定。

4.6.6 憑證中心公布已更新憑證

請參考第 4.6.1 章節規定。

4.6.7 憑證中心公告簽發憑證給其他單位

請參考第 4.6.1 章節規定。

4.7 憑證金鑰更換

4.7.1 憑證金鑰更換事由

請參考第 3.3 章節規定。

4.7.2 公鑰申請者

請參考第 3.3、4.1、4.2、4.3 及 4.4 章節規定。

4.7.3 憑證金鑰更換請求

請參考第 3.3、4.1、4.2、4.3 及 4.4 章節規定。

4.7.4 公告憑證簽發給憑證用戶

請參考第 3.3、4.1、4.2、4.3 及 4.4 章節規定。

4.7.5 已更換憑證金鑰的接受程序

請參考第 3.3、4.1、4.2、4.3 及 4.4 章節規定。

4.7.6 憑證中心公布已更換憑證金鑰

請參考第 3.3、4.1、4.2、4.3 及 4.4 章節規定。

4.7.7 憑證中心公告簽發憑證給其他單位

請參考第 3.3、4.1、4.2、4.3 及 4.4 章節規定。

4.8 憑證修正

4.8.1 憑證修正事由

本憑證中心不接受憑證修正，如憑證到期時，必須重新申請與舊憑證相同屬性的新憑證，重新申請時請參考第 4.1、4.2、4.3 及 4.4 章節規定。

4.8.2 憑證修正申請者

請參考第 4.8.1 章節規定。

4.8.3 憑證修正更換請求

請參考第 4.8.1 章節規定。

4.8.4 公告憑證修正給憑證用戶

請參考第 4.8.1 章節規定。

4.8.5 已修正憑證的接受程序

請參考第 4.8.1 章節規定。

4.8.6 憑證中心公布已修正憑證

請參考第 4.8.1 章節規定。

4.8.7 憑證中心公告簽發憑證給其他單位

請參考第 4.8.1 章節規定。

4.9 憑證廢止及暫時停用

4.9.1 憑證廢止之事由

(1) 憑證用戶申請廢止之事由：

- a. 憑證用戶因為控管措施的安全考量，欲廢止該憑證的使用，或憑證用戶擬不繼續使用憑證而廢止。
- b. 憑證內容及憑證用戶之相關註冊資訊有更動時。
- c. 與憑證相關的私密金鑰有毀損、遺失、曝露、被篡改，或有為第三者竊用之慮時。

(2) 本憑證中心得逕行廢止之事由：

- a. 因本憑證中心的金鑰變更、不適用、或因應系統整合需求。
- b. 本憑證中心的業務結束營運管理，而必須移轉至其他憑證機構的需求。
- c. 憑證用戶使用憑證而為本憑證中心/註冊窗口或主管機關(含合法授權之第三者)宣告未依據合約履行應盡義務或合約期滿，或不當使用憑證而有可能違反政府法律、規章、本作業基準之疑慮時。
- d. 憑證內容的憑證用戶相關資訊，與事實不符合時。

e. 憑證用戶之憑證未依本作業基準規定之作業程序簽發時。

f. 憑證用戶違反本作業基準或相關法令時。

(3) 權責單位：主管機關或法院，因業務之需求依照正式合法作業程序申請。

4.9.2 憑證廢止之申請者

(1) 欲廢止憑證之憑證用戶。

(2) 主管機關或合法授權之第三者。

4.9.3 憑證廢止之程序

(1) 個人身分之憑證用戶提出憑證廢止申請時，其程序如下：

- a. 個人身分之憑證用戶如因所屬之職務卸任或退休離職，則依據本院人員離職程序辦理憑證廢止。
- b. 非離職人員之憑證用戶，必須指派他人或親自擔任臨櫃申辦人，代表該憑證用戶至原申請憑證之註冊窗口申請憑證廢止。
- c. 註冊窗口依照第 3.2.2 章節規定，進行申辦人之身分鑑別程序，確認身分後，以公文書或電子表單方式函送本院資訊處，由註冊中心操作員經由網路連線至本憑證中心，線上廢止該憑證。

(2) 組織身分之憑證用戶提出憑證廢止申請時，其程序如下：

- a. 憑證用戶如為組織身分，則必須以該組織之名義，以公文書方式函送或由其指定代理人親至原申請憑證之註冊窗口辦理。
- b. 註冊窗口依照第 3.2.3 章節規定，針對申請資料進行身分鑑別程序，如資料正確無誤後，以公文書或電子表單方式函送本院資訊處，由註冊中心操作員經由網路連線至本憑證中心，線上廢止該憑證。

(3) 伺服器應用憑證之憑證用戶提出憑證廢止申請時，其程序如下：

- a. 憑證用戶必須以系統管理者身分提出憑證廢止申請，並以公文書或電子表單方式函送本院資訊處之註冊窗口辦理。
- b. 註冊窗口依照第 3.2.4 章節規定，針對申請資料進行身分鑑別程序，如資料正確無誤後，由註冊中心操作員經由網路連線至本憑證中心，線上廢止該憑證。

如以上之廢止申請審核不通過時，本憑證中心將拒絕廢止該憑證。

4.9.4 憑證廢止申請的處理期限

本憑證中心自註冊窗口受理憑證廢止申請日起，應於三個工作天內完成憑證廢止審核；註冊中心操作員於接受註冊窗口之審核確認公文後，一個工作天內完成憑證廢止作

業。

4.9.5 憑證中心處理憑證廢止時間

請參考第 4.9.4 章節規定。

4.9.6 憑證廢止查驗之規定

憑證用戶使用本憑證中心公布於儲存庫之憑證廢止清冊時，應先檢驗本憑證中心於憑證廢止清冊之數位簽章，以確認該憑證廢止清冊是否正確。

4.9.7 憑證廢止清冊之簽發頻率

憑證廢止清冊之簽發頻率為即時作業，更新後之憑證廢止清冊，將即時公布於儲存庫中，同時每天一次更新於本憑證中心網站。

4.9.8 憑證廢止清冊之最大潛在因素

不做規定。

4.9.9 線上憑證狀態查詢服務

本憑證中心提供線上憑證狀態協定(Online Certificate Status Protocol, OCSP)查詢服務。

4.9.10 線上憑證狀態查詢之規定

如憑證用戶無法依照第 4.9.6 章節之規定查詢憑證廢止清冊，則必須使用第 4.9.9 章節之查詢服務，查驗憑證用戶所使用的憑證是否有效。

4.9.11 其他形式廢止公告

不做規定。

4.9.12 金鑰被破解時之其他特殊規定

金鑰被破解時，請依照第 4.1、4.2、4.3 及 4.4 章節相關規定處理。

4.9.13 暫時停用憑證之事由

憑證用戶於憑證有效期間內，為保留憑證用戶的憑證使用權利，而不申請廢止憑證時，當有下述情況時，可執行暫時停用憑證：

(1) 請求暫時停用憑證之事由

- a. 憑證用戶的私密金鑰有可能遺失、洩露的不安全疑慮時，憑證用戶得提出暫時停用該憑證之使用。
- b. 憑證用戶欲暫時停止使用該憑證一段時間。

(2) 逕行暫時停用憑證之事由

- a. 憑證用戶使用憑證而為本憑證中心/註冊窗口或主管機關(含合法授權之第三者)宣告未依據合約履行應盡義務或合約期滿，或不當使用憑證而有可能違反政府法律、規章或本作業基準之疑慮時。

- b. 本憑證中心對於憑證用戶的私密金鑰有可能遺失、洩露的不安全疑慮時，得逕行暫時停用該憑證之使用。

4.9.14 暫時停用憑證之申請者

本憑證中心僅針對憑證用戶得提出暫時停用憑證之請求。暫時停用憑證之申請者如下：

- (1) 欲暫時停用憑證之憑證用戶。
- (2) 主管機關或合法授權之第三者。

4.9.15 暫時停用及恢復使用憑證之程序

- (1) 個人身分之憑證用戶得提出暫時停用憑證或恢復使用憑證之申請，其程序如下：
 - a. 個人身分之憑證用戶，必須指派他人或親自擔任臨櫃申辦人，代表該憑證用戶至註冊窗口，申請暫時停用憑證或恢復使用憑證。
 - b. 註冊窗口依照第 3.2.2 章節規定，進行臨櫃申辦人之身分鑑別程序，確認身分後，以公文書或電子表單方式函送本院資訊處，由註冊中心操作員經由網路連線至本憑證中心，線上暫時停用或恢復使用該憑證。
- (2) 組織身分之憑證用戶得提出暫時停用憑證或恢復使用憑證之申請，其程序如下：
 - a. 憑證用戶如為組織身分，則必須以該組織之名義，以公文書方式函送或由其指定代理人親至註冊窗口辦理。
 - b. 註冊窗口依照第 3.2.3 章節規定，針對申請資料進行身分鑑別程序，如資料正確無誤，以公文書或電子表單方式函送本院資訊處，由註冊中心操作員經由網路連線至本憑證中心，線上暫時停用或恢復使用該憑證。
- (3) 伺服器應用憑證之憑證用戶得提出暫時停用憑證或恢復使用憑證之申請，其程序如下：
 - a. 憑證用戶必須以系統管理者身分提出暫時停用憑證或恢復使用憑證之申請，並以公文書或電子表單方式函送或由其指定代理人親至註冊窗口辦理。
 - b. 註冊窗口依照第 3.2.4 章節規定，針對申請資料進行身分鑑別程序，如資料正確無誤，由註冊中心操作員經由網路連線至本憑證中心，線上暫時停用或恢復使用該憑證。

如以上之暫時停用憑證或恢復使用憑證之申請審核不通過時，本憑證中心將拒絕暫時停用或恢復使用該憑證。

4.9.16 暫時停用憑證的期間

本憑證中心不定義暫時停用憑證的期間，若暫時停用憑證之憑證用戶未提出恢復使用憑證之申請，則該憑證將持續被暫時停用。

4.9.17 暫時停用憑證的處理期限

本憑證中心自註冊窗口受理憑證暫時停用申請日起，應於三個工作天內完成憑證暫時停用審核；註冊中心操作員於接受註冊窗口之審核確認公文後，一個工作天內完成憑證暫時停用作業。

4.10 憑證狀態查詢服務

4.10.1 查詢憑證運作特性

請參考第 4.9.9、4.9.11 及 4.9.13 章節規定。

4.10.2 查詢憑證適用性

請參考第 4.9.9、4.9.11 及 4.9.13 章節規定。

4.10.3 查詢憑證附加功能

請參考第 4.9.9、4.9.11 及 4.9.13 章節規定。

4.11 簽發終止

當本憑證中心所簽發的憑證到期或本憑證中心停止營運時，已簽發的憑證皆失效。

4.12 金鑰託管與復原

4.12.1 金鑰託管與復原策略與實作

請參考第 6.2.3 章節規定。

4.12.2 會議金鑰封裝與復原策略與實作

不做規定。

5 非技術性安全控管

5.1 實體管控

5.1.1 實體所在及結構

本憑證中心機房位於本院資訊處，符合儲存高重要性及敏感性資訊的機房設施水準，並具備門禁、保全及監視錄影等實體安全機制，以防止未經授權存取本憑證中心之相關設備。

5.1.2 實體存取

- (1) 機房之實體控管運作，採取符合本院資訊安全管理標準之安全控管措施，以防止未經授權存取硬體、軟體和硬體密碼模組等相關設備。
- (2) 機房入口處及管制區域設有門禁讀卡機，須讀卡方能進入，僅有被授權的人員才得以進入，訪客必須經過授權的人引導進入，進入此區域的授權人數應保持最少。
- (3) 本憑證中心相關人員離開機房時，將進行以下之查驗工作並記錄，以防止未授權人員進入機房：
 - a. 確認設備是否正常運作。
 - b. 確認機櫃門是否關閉。
 - c. 確認門禁系統是否正常運作。

5.1.3 電力及空調系統

- (1) 本憑證中心的電力系統，除市電外，另設有發電機及不中斷電源系統(UPS)，並具有市電及發電機的電源自動切換功能，以避免停電所造成的不正常關機。
- (2) 本憑證中心的環境建置，具有空調系統來控制溫度與溼度，且與大樓空調獨立，使機房保持最佳運作環境。

5.1.4 水源干擾

本憑證中心設於免於水災之處所，雨水無法進入，且樓層裝置高架地板無進水之疑慮。

5.1.5 防火設施

本憑證中心機房具備自動偵測火災預警功能，在本憑證中心的操作範圍內，均安置適當的滅火設備，以因應可能的火災。

5.1.6 儲存媒介

媒體儲存環境，具有實體保護措施，其中一份備份資訊的儲存媒體具有安全控管措施。

5.1.7 廢棄物處理

在本憑證中心內，有關系統的紙張文件，或是電子文件中包含認證的元件，必須藉

由以下各方法加以安全地處理廢棄物：

(1) 電子文件方面：

- a. 透過物理性實體破壞，將實體物件完全損毀。
- b. 利用適當的應用程式將資料覆蓋或刪除。

(2) 印出的文件則須經過絞碎或是焚毀的方式來安全處理。

5.1.8 異地備援

在本院新店異地備援中心儲存所有軟體及資料的備份。

5.2 作業程序控管

5.2.1 信任規則

為了確保一個人無法操作全部的系統，本憑證中心管理者的責任可藉由多個信賴角色來分擔。因此在本憑證中心，必須有不同的人來擔任不同的信賴角色，每個人應有一定的權限，此方式將允許系統在不同角色間，進行檢查與相互平衡。

本憑證中心的信賴角色分為「管理人員」、「金鑰保管人員」、「稽核人員」、「維運人員」四種角色，每種信賴角色將依照第 5.3 章節規定進行人員控管，以防止可能的內部攻擊。四種信賴角色的工作說明如下：

(2) 管理人員：

- a. 負責系統安裝、管理作業及環境參數之設定。
- b. 建立和維護註冊中心操作員之帳號。
- c. 產製和備份本憑證中心之金鑰。

(3) 金鑰保管人員：負責保管本憑證中心之私密金鑰 IC 分持卡。

(4) 稽核人員負責：

- a. 對稽核紀錄之查驗、維護和歸檔。
- b. 執行或監督內部的稽核，以確認本憑證中心運作，是否遵照本作業基準的規定。

(5) 維運人員負責：

- a. 負責憑證簽發、廢止及廢止清冊之公告。
- b. 系統設備的日常運作維護。
- c. 儲存媒體的更新。
- d. 系統的實體安全控管(機房的門禁管理、防火、防水及空調系統等)。

5.2.2 每項工作所需的人數

本憑證中心目前於「信賴角色」中，所述各角色的配置人力均為一人，且為分離的獨立個體，以提供系統運作之最大安全保證。但是角色分派必須符合以下規定：

- (1) 管理人員、金鑰保管人員，以及稽核人員三種信賴角色不得相互兼任，但可兼任維運人員。
- (2) 任何一種信賴角色均不允許執行自我稽核功能。

5.2.3 角色的識別與驗證

負責本憑證中心維運作業的人員，均配發貼有近期照片的專屬證件作為實體的識別。擔任「信賴角色」中，所述及的維運人員於進行系統維運作業時，須以憑證或帳號/密碼進行系統登入，以識別維運人員的身分。

5.3 人員控管

5.3.1 適任條件與經歷

- (1) 負責本憑證中心執行各種業務的作業人員，必須具備忠實、可信賴及工作的熱誠度，無影響憑證作業之其他兼職工作，無憑證作業上因工作之疏失、不盡責之缺失紀錄，無違法犯紀之不良紀錄。
- (2) 管理人員與稽核人員，至少具備憑證作業的實務經驗，具有電腦系統規劃、開發、營運管理的經驗更佳，並由本院資訊處選派適當人員擔任。
- (3) 維運人員，至少具備憑證作業的實務經驗，或經過憑證相關作業之訓練而通過測驗者，並由本院資訊處選派適當人員擔任。

5.3.2 背景調查過程

本憑證中心各種相關角色人員，在進用前予以資格審查，以確認其身分資格相關證明文件是否屬實。

5.3.3 教育訓練

本憑證中心的相關人員，依照其職務需求，施予憑證系統運作所應具備的資訊安全教育與系統運作訓練，以減少人為錯誤或威脅所造成系統的損害。每年定期評估其相關知識與技能，施予適當之再教育訓練，以確保本憑證中心維運作業的品質。

5.3.4 職位調動的頻率及順序

本憑證中心目前暫不對維運作業人員實施工作輪調機制。

5.3.5 未授權行動的制裁

本憑證中心的相關人員，若於執行維運作業時，發生違反憑證政策及相關作業規定時，將接受適當檢討，若情節重大對本憑證中心的維運造成影響者，將採取法律行動追究責任，並要求損害賠償。

5.3.6 約聘人員的規定、人事合約的需求

本憑證中心若須進行人員約聘，約聘人員應簽署保密協定且必須為全職人員，同時約聘人員應接受其執行業務所需之足夠教育訓練，以利其業務之執行。

5.3.7 文件資料的提供

本憑證中心的維運作業人員可存取以下相關資訊：

- (1) 硬體及軟體文件。
- (2) 本憑證中心文件：
 - a. 應用手冊。
 - b. 政策文件(包括本作業基準)。
 - c. 操作程序文件。

5.4 安全稽核程序

5.4.1 被記錄事件種類

被記錄的事件可分為實體事件與邏輯事件兩大類，實體事件紀錄可使用電子媒體或書面形式為之；邏輯事件則為與憑證管理系統運作相關的系統事件，並由系統自動記錄。

- (1) 實體事件
 - a. 機房的人員出入。
 - b. 機房設施的出入變動。
 - c. 本憑證中心的憑證管理系統之實體存取。
- (2) 邏輯事件
 - a. 憑證註冊紀錄。
 - b. 產生憑證請求。
 - c. 憑證公告紀錄，包括憑證廢止清冊。
 - d. 稽核紀錄包括安全相關事件。
 - e. 憑證廢止紀錄。

5.4.2 處理紀錄的頻率

- (1) 本憑證中心至少每半年檢視一次稽核紀錄，檢視是否有異常紀錄產生。
- (2) 檢視工作包括檢視所有紀錄項目及檢查任何警示或異常等。
- (3) 檢視稽核紀錄之結果以書面文件記錄。

5.4.3 稽核紀錄保留期限

本憑證中心之稽核紀錄現場保留兩個月，並依照第 5.4.4、5.4.5、5.4.6、5.5 章節管理

機制等相關規定辦理。

如稽核紀錄檔的保留期限屆滿，在稽核員的監督下，由維運人員負責移除資料。

5.4.4 稽核紀錄的保護

- (1) 本憑證中心的實體事件稽核紀錄，將存放於安全處所，經授權的系統管理人員，與經授權的系統管理人員陪同的合格稽核員，方有權限存取。
- (2) 本憑證中心的邏輯事件稽核紀錄，將使用金鑰進行簽署，以確保稽核紀錄之完整性。邏輯事件稽核紀錄存取，亦須經授權的系統管理人員，與經授權的系統管理人員陪同的合格稽核員，方有權限為之。

5.4.5 稽核紀錄備份程序

本憑證中心的邏輯事件稽核紀錄，將定期執行備份作業，以確保紀錄安全。

5.4.6 安全稽核系統

稽核系統內建於本憑證中心的系統，稽核程序在本憑證中心系統啟動時啟用，唯有在本憑證中心系統關閉時才停止。

5.4.7 對引起事件者之告知

如因發生事件而被稽核系統記錄，稽核系統並不需要告知引起該事件的個體，其所引發的事件已經被系統記錄。

5.4.8 弱點評估

除稽核紀錄之處理外，本憑證中心定期執行系統環境之弱點評估，進行改善。

5.5 紀錄歸檔方法

5.5.1 紀錄事件之類型

- (1) 本憑證中心的憑證政策。
- (2) 本憑證中心的系統架構與組態資料。
- (3) 本憑證中心的稽核資料。
- (4) 憑證申請資料。
- (5) 憑證廢止資料。
- (6) 已簽發的憑證。
- (7) 本憑證中心簽發的憑證廢止清冊。
- (8) 本憑證中心維運相關的文件資料。
- (9) 憑證作業相關的組織與身分鑑別資料。

5.5.2 歸檔之保留期限

- (1) 金鑰的安全維護：加密金鑰備份檔案的保存至少十年或是另有其他規定考量。

(2) 憑證的安全維護：本憑證中心及註冊中心的憑證應建檔，並保存至少十年或是另有其他規定考量。

(3) 檔案維護的期限：稽核追蹤紀錄應保存至少十年或是另有其他規定考量。

5.5.3 歸檔之保護

(1) 不允許新增、修改或刪除歸檔資料。

(2) 本憑證中心將歸檔資料以實體加以保護，或是結合實體與加密方式保護，同時也考量環境因素(溫度與溼度的隔離等等)。

5.5.4 歸檔之備份程序

本憑證中心將金鑰與憑證等相關資料，依照備份與備援回復作業程序，分為本院本地端機房內之歸檔備份及新店異地備援中心之歸檔備份。

本地端：每日(星期一至星期日)進行完整備份於本地磁帶機上。

異地端：採不定期完整備份，並於必要時進行差異備份，使用安全的加密通道進行備份資料的傳輸，保存資料儲存於具安全管控措施的異地備援環境。

5.5.5 紀錄之時戳要求

系統紀錄的時戳部分，由於時間來源為系統硬體，故系統操作人員應確保系統時間的正確性，以維系統紀錄其時戳的有效性。書面紀錄亦將記載日期資訊，必要時並將記載時間資訊。書面紀錄的日期與時間紀錄不可任意更改，如需更改必須由稽核員簽名確認。

5.5.6 歸檔資料彙整系統

不做規定。

5.5.7 歸檔紀錄之取得及驗證程序

(1) 必須以書面申請獲得正式授權後，才可取得歸檔資料。

(2) 由稽核員負責驗證歸檔資料，並驗證文件簽署者及日期等之真偽。

5.6 金鑰更換

(1) 本憑證中心將於自簽憑證用的私密金鑰到期前三個月，更換用來簽發憑證的金鑰對，並簽發一張有效的自簽憑證。

(2) 本憑證中心的憑證用戶，若需持續使用本憑證中心所簽發的憑證，可於其憑證到期前三個月，由本憑證中心代為提出新憑證申請，以取代舊憑證。

(3) 金鑰更換應由手動產生，且在本憑證中心的階層架構下，不存在自動更換金鑰的程序。

5.7 金鑰遭破解或災變時之復原程序

5.7.1 電腦資源、軟體、資料被竄改

- (1) 本憑證中心訂定電腦資源、軟體及資料遭破壞之復原程序，同時每年進行演練。
- (2) 本憑證中心的電腦資源、軟體、或資料遭毀損時，如系統簽發憑證用的金鑰未受損毀，則利用備份資料回復本憑證中心的儲存庫服務，並提供外界憑證下載及憑證有效性查詢的管道，接著重新建立憑證簽發與憑證管理的能力。
- (3) 若系統簽發憑證用的金鑰損毀，則本憑證中心將利用備份的金鑰資料進行金鑰回復。

5.7.2 金鑰憑證被廢止之復原程序

本憑證中心的簽章金鑰憑證被廢止時，本憑證中心將重新產製金鑰對，並重新簽發自簽憑證及所有憑證，將所有新的憑證公布在儲存庫中，同時公告或通知憑證用戶更換憑證。

5.7.3 金鑰憑證遭破解之復原程序

本憑證中心自身的私密金鑰有危害之疑慮時，本憑證中心將重新產製金鑰對，並重新簽發自簽憑證及所有憑證，將所有新憑證公布在儲存庫中，同時公告或通知憑證用戶更換憑證。

5.7.4 安全設施之災後復原工作

本憑證中心之系統運作所使用的相關安全設施，若因災害發生而致毀損時，則依以下程序處理：

- (1) 在不會影響憑證管理系統運作前，儘速修護或更新相關安全設施至正常運轉狀態。
- (2) 當足以造成憑證管理系統運作的危害時，必須立刻緊急關閉憑證管理系統的運作，且儘速修護或更新相關安全設施至正常運轉狀態，才開啟憑證管理系統運作。如果於作業規範的時間內，無法修護或更新相關安全設施時，本憑證中心將於異地正式啟動備援機制。
- (3) 如發生的災害已嚴重損害憑證管理系統運作所使用的相關安全設施時，則必須執行異地備援計畫，以回復本憑證中心的運作功能。

5.8 憑證中心終止服務

本憑證中心終止服務時，將依據電子簽章法相關規定辦理。本憑證中心將遵守以下事項，以確保終止服務對於憑證用戶與信賴憑證者造成之影響最小：

- (1) 本憑證中心於預定終止服務三十日前，應通知電子簽章法主管機關。
- (2) 本憑證中心於終止服務之日三十日前，將終止服務及由其他憑證機構承接之事實

通知憑證用戶。

(3) 本憑證中心終止服務時將採以下措施：

- a. 停止簽發新的憑證。
- b. 於安全之作業環境下，廢止本憑證中心與全部的憑證。
- c. 將本憑證中心之相關私密金鑰與憑證、全部的憑證與憑證廢止清冊，移轉至承接的憑證機構。
- d. 將所有營運期間之紀錄檔案，移交給承接此業務之其他憑證機構。

6 技術安全控管

6.1 本憑證中心金鑰對之產製與安裝

6.1.1 金鑰對之產製

- (1) 本憑證中心的金鑰在通過 FIPS 140-1(含)以上認證的硬體密碼模組(Hardware Security Module, HSM)內進行金鑰對的安全產製，採 RSA 金鑰演算法，私密金鑰在硬體密碼模組內產製後，受此硬體密碼模組保護而不外洩。
- (2) 如憑證用戶使用之憑證載具為 IC 卡時，則其金鑰對是由註冊中心操作員代為產製，註冊中心操作員採用通過 CC(Common Criteria)標準 EAL4(含)以上等級認證或安全強度相當的 IC 卡，並在 IC 卡內部產製金鑰對。
- (3) 如憑證用戶使用其他憑證載具時，則可授權由註冊中心操作員代為產製金鑰對，或由憑證用戶自行產製金鑰對及控管，憑證用戶需採取適當之安控措施，並於申請憑證時確保私密金鑰管理之安全性。

6.1.2 私密金鑰之安全遞送

- (1) 本憑證中心自身的私密金鑰為自行產製，故無私密金鑰遞送之需要。
- (2) 如憑證用戶私密金鑰由註冊中心操作員代為產製時，註冊窗口將於本憑證中心簽發憑證後，通知憑證用戶臨櫃領取存有私密金鑰的 IC 卡。

6.1.3 公鑰遞送給本憑證中心

- (1) 如憑證用戶之金鑰對由註冊中心操作員代為產製時，則由註冊中心透過安全管道將憑證用戶之公開金鑰傳送至本憑證中心。
- (2) 如憑證用戶自行產製金鑰對時，則憑證用戶必須以憑證申請檔的格式，將公開金鑰送給註冊中心，註冊中心依照第 3.2.1 章節規定檢驗憑證用戶，確實擁有相對應的私密金鑰後，以安全管道將憑證用戶的公開金鑰傳送至本憑證中心。

6.1.4 憑證中心公鑰傳送給憑證用戶

本憑證中心於網站上(<http://ca.ly.gov.tw>)，公布本憑證中心自簽憑證，且提供識別資訊與驗證完整性資料(憑證拇指紋)，同時提供憑證用戶或信賴憑證者進行查詢或下載作業。

信賴憑證者在使用本憑證中心的自簽憑證前，必須使用本憑證中心自簽憑證上的公開金鑰，檢驗自簽憑證之簽章，以確保本憑證中心的公開金鑰是可被信賴的。

6.1.5 金鑰長度

- (1) 本憑證中心使用 2048 位元(含)以上的 RSA 金鑰簽發憑證及憑證廢止清冊。
- (2) 憑證用戶使用 1024 位元(含)以上的 RSA 金鑰。

6.1.6 公開金鑰參數的產生

- (1) 本憑證中心依照第 6.2.1 章節規定，使用通過 FIPS 140-1(含)以上安全認證的硬體

密碼模組產製亂數、公開金鑰對和對稱金鑰。

- (2) 憑證用戶使用通過 CC(Common Criteria)標準 EAL4 等級認證或安全強度相當的 IC 卡，並由 IC 卡內部產製金鑰對；或使用其他軟硬體密碼模組產製金鑰對。

6.1.7 參數品質的檢核

本憑證中心的 RSA 公開金鑰參數品質，由通過 FIPS 140-1 驗證標準，安全等級為 Level 4 的硬體密碼模組檢核。

6.1.8 金鑰經軟體或硬體產製

- (1) 本憑證中心自身的金鑰於通過 FIPS 140-1 驗證標準，安全等級為 Level 4 的硬體密碼模組內直接產製。
- (2) 憑證用戶使用通過 CC(Common Criteria)標準 EAL4 等級認證或安全強度相當的 IC 卡，並在 IC 卡內部產製金鑰對；或使用其他軟硬體密碼模組產製金鑰對。

6.1.9 金鑰之使用目的

- (1) 本憑證中心之憑證金鑰用途為 Digital Signature、Non-Repudiation、Certificate Signing、Off-line CRL Signing、CRL Signing。
- (2) 本憑證中心簽發給憑證用戶，作為簽章或加密用途的憑證，其用途訂定於 X.509 v.3 憑證的金鑰用途欄位，憑證用戶必須依照本作業基準與業務應用系統的規範，使用於相關業務上。

6.2 私密金鑰的保護

6.2.1 標準密碼模組

本憑證中心與註冊中心使用通過 FIPS 140-1 安全認證的硬體密碼模組；憑證用戶金鑰對之儲存媒體可為 IC 卡或其他載具。

6.2.2 私密金鑰的分持控管

本憑證中心自身的私密金鑰，均安全地存放在硬體密碼模組中，並由硬體密碼模組所控管，本憑證中心金鑰分持採用機密分持(secret splitting)m-out-of-n 方式，可做為私密金鑰分持備份及回復方法。

6.2.3 私密金鑰的託管

本憑證中心自身的私密金鑰不受任何機構託管，同時也不負責保管憑證用戶之簽章用的私密金鑰。

6.2.4 私密金鑰的備份

- (1) 本憑證中心依照第 6.2.2 章節之金鑰分持控管方法備份自身的私密金鑰，並使用高安全性的 IC 卡做為秘密分持的儲存媒體。
- (2) 註冊中心操作員於產製憑證用戶的金鑰對時，針對憑證用戶之解密用的私密金鑰進行備份。

6.2.5 私密金鑰的歸檔

- (1) 本憑證中心自身之簽章用的私密金鑰不可以被歸檔，本憑證中心也不負責保管憑證用戶之簽章用的私密金鑰。
- (2) 憑證用戶之解密用的私密金鑰，由註冊中心操作員於產製金鑰時，透過憑證管理系統完成歸檔作業。

6.2.6 私密金鑰輸入至密碼模組

本憑證中心只有在進行金鑰備份回復時，才可將私密金鑰輸入至密碼模組中。

6.2.7 私密金鑰的啟用

- (1) 本憑證中心之 RSA 私密金鑰之啟動(Activation)，是以 m-out-of-n 控管 IC 卡組進行控制，不同用途的控管 IC 卡組由金鑰保管人員保管。
- (2) 憑證用戶之私密金鑰儲存於其 IC 卡時，採用 IC 卡 PIN 碼做為啟用資料，在啟用私密金鑰時，必須由憑證用戶輸入 PIN 碼。
- (3) 憑證用戶使用其他密碼模組時，私密金鑰之啟動方式，可使用之認證鑑別方式包含(但不限於)通行詞組(Pass-Phrase)、個人符記、個人識別(PIN)或生物識別。但輸入的啟動資料必須避免被洩漏。

6.2.8 私密金鑰的停用

- (1) 本憑證中心的 RSA 私密金鑰之停用，是以多人授權控管的手動方式進行控制。
- (2) 憑證用戶在使用 IC 卡中的私密金鑰時，若輸入 PIN 碼錯誤超過三次時，則該 IC 卡將會因 PIN 碼被鎖碼(Block)而遭停用。被鎖碼的 IC 卡必須經本院資訊處解鎖(Unblock)並重設 PIN 碼後才能繼續使用。
- (3) 憑證用戶使用其他密碼模組時，私密金鑰之停用方式可透過手動的移除程序，或經過一段時間沒有運作後自動停止運作。

6.2.9 私密金鑰的回復

- (1) 本憑證中心自身的私密金鑰備份回復，請參考第 6.2.6 章節規定。
- (2) 憑證用戶之解密用的私密金鑰，其備份回復之程序與申請憑證之程序相同，請參考第 4.2 章節規定，憑證用戶於填寫申請表後，經原憑證之註冊窗口審核完成，最後由註冊中心操作員代為回復其解密用的私密金鑰。

6.2.10 私密金鑰的銷毀

- (1) 本憑證中心自身的私密金鑰於效期屆滿後，將予歸檔保存於安全處所，並不進行銷毀。
- (2) 憑證用戶之私密金鑰儲存於其 IC 卡中，當憑證用戶更換新的 IC 卡或不再繼續使用時，且憑證用戶確定不再需要使用該 IC 卡對檔案或訊息進行解密時，憑證用戶須將該 IC 卡繳回，並由本憑證中心進行私密金鑰之銷毀。

- (3) 憑證用戶使用其他密碼模組時，軟體密碼模組之私密金鑰銷毀必須以資料覆蓋方式(Overwrite)清除。

6.3 用戶金鑰對管理之其他規定

6.3.1 公開金鑰的歸檔

本憑證中心將進行憑證之歸檔，且依照規定執行歸檔系統之安全控管，不再另外進行公開金鑰之歸檔。

6.3.2 公開金鑰及私密金鑰的有效期限

- (1) 本憑證中心自身的公開金鑰及私密金鑰之金鑰長度為 RSA 2048 位元，公開金鑰與私密金鑰之使用期限至多均為 25 年。
- (2) 憑證的公開金鑰與私密金鑰，其有效期限說明如下：立法委員憑證有效期限為 4 年、公費助理憑證有效期限為 4 年、職員憑證有效期限為 8 年、伺服器應用憑證有效期限為 10 年、外包廠商憑證有效期限為 1 年(或因專案需求彈性調整，最長期限以 2 年為限)、外單位憑證有效期限為 1 年、院內單位臨時憑證有效期限為 8 年、傳播媒體憑證有效期限為 1 年。

6.4 啟動資料

6.4.1 啟動資料的產生與安裝

本憑證中心的啟動資料是由硬體密碼模組產生，再寫入至 m-out-of-n 控管 IC 卡組中，IC 卡中的啟動資料將由硬體密碼模組內建的讀卡機直接存取，IC 卡的 PIN 碼直接在硬體密碼模組內建的鍵盤上輸入。

本憑證中心的啟動資料，主要分成兩大部份：

- (1) HSM：存放本憑證中心所有元件的私鑰，並藉由控管 IC 卡，來啟動 HSM 的服務。
- (2) 憑證系統啟動：藉由系統服務來管理本憑證中心各個元件(CA,RA...等)的啟動。

6.4.2 啟動資料的保護

本憑證中心的啟動資料由 m-out-of-n 控管 IC 卡組保護，IC 卡的 PIN 碼由金鑰保管人員負責保存，不得記錄於任何媒體上，如登入的失敗次數超過三次，則鎖住此 IC 卡；IC 卡移交時，新的保管人員必須重新設定新的 PIN 碼。

6.4.3 啟動資料的其他考量

本憑證中心自身的私密金鑰，其啟動資料不做歸檔。

6.5 電腦安全控管

6.5.1 特定電腦安全技術需求

本憑證中心依據本院資訊安全管理規範施行及運作，本憑證中心的系統安控措施，包含下列作業：

- (1) 具備身分的識別及驗證管控機制。
- (2) 提供系統資源及資料庫存取權限控管。
- (3) 提供安控事件的紀錄。
- (4) 具備資料備份與保存的保護措施。
- (5) 人員權責區分。
- (6) 內部作業程序控管。
- (7) 具備業務永續經營回復機制。
- (8) 具備信賴角色和相關身分識別的安全及可信賴的管道。
- (9) 具備程序完整性及安全控管保護。

6.5.2 電腦系統安全等級

本憑證中心採用安全強度與 CC(Common Criteria)標準 EAL4 等級相當的電腦作業系統。

6.6 生命週期技術控管措施

6.6.1 系統開發控管措施

本憑證中心的軟體開發作業控管規範，依據 ISO 15408 共通標準(Common Criteria)等級的規範執行，或類似此 ISO 共通標準等級的軟體開發控管規範，執行相關系統規劃與開發的作業控管。

6.6.2 安全管理控管措施

本憑證中心系統在首次安裝時，將確認是由供應商提供正確的版本且未被修改。本憑證中心將記錄和控管系統的組態及任何修正與功能的提升。

6.6.3 生命週期安全等級

不做規定。

6.7 網路安全管控

- (1) 本憑證中心的主機與內部儲存庫，透過雙重防火牆和外部網路連接，除必要的維護或備援外，提供不中斷的憑證與憑證廢止清冊查詢服務。
- (2) 憑證管理系統的安裝主機與儲存庫，透過系統弱點掃描，執行必要修補程式之安裝。

6.8 密碼模組工程的管控

請參考第 6.1 及 6.2 章節規定。

7 憑證及憑證廢止清冊的剖繪

7.1 憑證的剖繪

本憑證中心簽發的憑證之格式剖繪，依照本基礎建設憑證及憑證廢止清冊格式剖繪相關規定。

7.1.1 版本號碼

本憑證中心簽發 X.509 v.3 版本的憑證。

7.1.2 憑證擴充欄位

本憑證中心支援 X.509 v.3 的憑證延伸部分，憑證擴充欄位依照憑證政策等相關規定。

7.1.3 演算法的物件識別代碼

本憑證中心所使用的演算法物件識別代碼，為 ISO 物件識別代碼(OID)管理單位公告的規範。

(1) 支援下面雜湊及訊息摘要的演算法：

演算法安全機制	演算法(Algorithm)	物件識別代碼(OID)
雜湊函數	SHA-1	1.3.14.3.2.26
雜湊函數	MD5	1.2.840.113549.2.5

(2) 支援以下加密封裝的演算法：

演算法安全機制	演算法(Algorithm)	物件識別代碼(OID)
簽章	signature scheme	1.3.36.3.4
簽章	SHA-1 with RSA Encryption	1.2.840.113549.1.1.5

(3) 支援以下加密的演算法：

演算法安全機制	演算法(Algorithm)	物件識別代碼(OID)
亂碼	RSASignature	1.2.840.113549.1.1.1
亂碼	DesCBC	1.3.14.3.2.7
亂碼	3desEDE-CBC	1.2.840.113549.3.7

7.1.4 命名形式

憑證的主體與簽發者兩個欄位值，使用 X.500 的唯一識別名稱，此名稱的屬性型態遵循 RFC 3280 相關規定。

7.1.5 命名限制

本憑證中心簽發之憑證，不使用命名限制。

7.1.6 憑證政策物件識別碼

本憑證中心均依 X.509 v.3 規範簽發憑證，憑證政策相關的物件識別碼(OID)，存放於憑證內憑證政策相關的識別欄位。

7.1.7 憑證政策限制擴充欄位的使用

本憑證中心簽發之憑證可視需要，包含政策限制(policyConstraints)之擴充欄位。

7.1.8 憑證政策限定元的語法及語意

本憑證中心簽發之憑證，不含政策限定元(policyQualifier)。

7.1.9 關鍵憑證政策擴充欄位的語意處理

本憑證中心簽發之憑證，所含的憑證政策擴充欄位，不註記為關鍵擴充欄位。

7.2 憑證廢止清冊的剖繪

本憑證中心簽發的憑證廢止清冊之格式剖繪，依照本基礎建設憑證及憑證廢止清冊格式剖繪相關規定。

7.2.1 版別號碼

本憑證中心簽發 X.509 v.2 版本的憑證廢止清冊。

7.2.2 憑證廢止清冊與憑證廢止清冊的擴充欄位

本憑證中心簽發的憑證廢止清冊依照憑證政策相關規定。

8 憑證實務作業基準之維護

8.1 本作業基準之生效與終止

8.1.1 本作業基準之生效

本作業基準公告於本憑證中心網站(<http://ca.ly.gov.tw>)，本作業基準之生效日期，除另有規定外，於公告時生效。

8.1.2 本作業基準之終止

本作業基準經電子簽章法主管機關核定後，除非有新版的本作業基準，本作業基準將不會終止。

8.1.3 本作業基準之終止的影響

當本作業基準終止時，其已發行的憑證仍然有效，除非憑證有效日期已達截止日期時，該憑證即為無效。

8.2 本作業基準之變更程序

本作業基準每年定期評估是否需要修訂，以維持其保證度。修訂方式包括以附加文件方式修訂及直接修訂本作業基準的內容。如憑證政策修訂或物件識別碼變更時，本作業基準將配合修訂。

8.2.1 變更時不另作通知之變更項目

本作業基準重新排版時，不另作通知。

8.2.2 應通知之變更項目

本憑證中心每年至少一次審查本作業基準，確保符合主管機關規範的要求；或因配合業務需求、憑證管理系統架構與功能的調整、國際標準規範更新、作業錯誤及憑證用戶適當之建議，而適當修改本作業基準的內容，確保本作業基準的適用性。

(1) 政策的變更包含以下：

- a. 本作業基準的新版發行。
- b. 改變或替換現存的政策。

(2) 當本作業基準訂定相關的物件識別代碼(OID)，而本作業基準內容有更新版本時，相對應的物件識別代碼不跟隨異動，只變更版本的序號識別代碼。

8.3 本作業基準之公布及通知程序

新的或是更正過的本作業基準，經主管機關審查通過後，公布在本憑證中心網站(<http://ca.ly.gov.tw>)。

8.4 本作業基準之核准程序

本作業基準的主管機關為經濟部，並依據及受政府與主管機關訂定的電子簽章法、電子簽章法施行細則、憑證實務作業基準應載明事項之管轄與監督，且須經主管機關的

核定。