HiPKI 憑證總管理中心

憑證實務作業基準

(HiPKI Root Certification Authority

Certification Practice Statement)

第 1.1 版

中華電信股份有限公司

中華民國 109 年 7 月 2 日

目　　錄

1 序論.....1

1.1 概要.....1

1.1.1 憑證實務作業基準.....1

1.1.2 憑證實務作業基準之適用範圍.....3

1.2 文件名稱及識別.....3

1.3 主要成員.....6

1.3.1 憑證機構.....6

1.3.2 註冊中心.....8

1.3.3 用戶.....8

1.3.4 信賴憑證者.....8

1.3.5 其他相關成員.....8

1.4 憑證用途.....9

1.4.1 憑證之適用範圍.....9

1.4.2 憑證之禁用範圍.....10

1.5 政策管理.....11

1.5.1 憑證實務作業基準之管理機構.....11

1.5.2 聯絡資料.....11

1.5.3 憑證實務作業基準之審定.....12

1.5.4 憑證實務作業基準之核准程序.....12

1.6 名詞定義及縮寫.....13

1.6.1 名詞定義.....13

1.6.2 縮寫.....25

2 公布及儲存庫之責任.....28

2.1 儲存庫.....28

2.2 憑證機構之資訊公布.....28

2.3 公布之時間或頻率.....29

2.4 儲存庫之存取控制.....29

3 識別及鑑別.....30

3.1 命名.....30

3.1.1 命名種類 30
3.1.2 命名須有意義 30
3.1.3 用戶之匿名或假名 30
3.1.4 不同命名形式之解釋規則 30
3.1.5 命名之獨特性 30
3.1.6 商標之辨識、鑑別及角色 31
3.2 初始身分驗證 31
3.2.1 證明擁有私密金鑰之方式 31
3.2.2 組織身分鑑別 31
3.2.3 個人身分鑑別 33
3.2.4 未經驗證之用戶資訊 33
3.2.5 授權之確認 33
3.2.6 互運之準則 34
3.2.7 資料來源正確性 34
3.3 金鑰更換請求之識別及鑑別 35
3.3.1 例行性金鑰更換之識別及鑑別 35
3.3.2 憑證廢止後金鑰更換之識別及鑑別 35
3.4 憑證廢止請求之識別及鑑別 35
4 憑證生命週期營運規定 36
4.1 憑證申請 36
4.1.1 憑證之申請者 36
4.1.2 註冊程序及責任 36
4.2 憑證申請之程序 39
4.2.1 執行識別及鑑別 39
4.2.2 憑證申請之批准或拒絕 40
4.2.3 處理憑證申請之時間 41
4.3 憑證簽發 41
4.3.1 憑證簽發時憑證機構之作業 41
4.3.2 憑證機構對憑證申請者之憑證簽發通知 42
4.4 憑證接受 42
4.4.1 構成接受憑證之事由 42
4.4.2 憑證機構對簽發憑證之發布 42
4.4.3 憑證機構對其他個體之憑證簽發通知 43
4.5 金鑰對及憑證之用途 43

4.5.1 用戶私密金鑰及憑證之用途 43
4.5.2 信賴憑證者公開金鑰及憑證之用途 43
4.6 憑證展期 44
4.6.1 憑證展期之情況 44
4.6.2 憑證展期之申請者 44
4.6.3 憑證展期之程序 44
4.6.4 對用戶憑證展期之簽發通知 44
4.6.5 構成接受展期之憑證的事由 45
4.6.6 憑證機構對展期之憑證的發布 45
4.6.7 憑證機構對其他個體之憑證簽發通知 45
4.7 憑證機構憑證之金鑰更換 45
4.7.1 憑證金鑰更換之情況 45
4.7.2 更換憑證金鑰之申請者 46
4.7.3 憑證金鑰更換之程序 46
4.7.4 對憑證機構憑證金鑰更換之簽發通知 46
4.7.5 構成接受金鑰更換之憑證的事由 46
4.7.6 憑證機構對金鑰更換之憑證的發布 47
4.7.7 憑證機構對其他個體之憑證簽發通知 47
4.8 憑證變更 47
4.8.1 憑證變更之情況 47
4.8.2 憑證變更之申請者 47
4.8.3 憑證變更之程序 47
4.8.4 對憑證機構憑證變更之簽發通知 47
4.8.5 構成接受變更之憑證的事由 47
4.8.6 憑證機構對變更之憑證的發布 48
4.8.7 憑證機構對其他個體之憑證簽發通知 48
4.9 憑證廢止及停用 48
4.9.1 憑證廢止之情況 48
4.9.2 憑證廢止之申請者 49
4.9.3 憑證廢止之程序 50
4.9.4 憑證廢止請求之寬限期 51
4.9.5 憑證機構處理憑證廢止請求之處理期限 51
4.9.6 信賴憑證者檢查憑證廢止之規定 51
4.9.7 憑證廢止清冊之簽發頻率 52
4.9.8 憑證廢止清冊發布之最大延遲時間 53
4.9.9 線上憑證廢止及狀態查驗之可用性 53

4.9.10 線上憑證廢止查驗之規定 53
4.9.11 廢止公告之其他發布形式 54
4.9.12 金鑰被破解時之特殊規定 55
4.9.13 憑證停用之情況 55
4.9.14 憑證停用之申請者 55
4.9.15 憑證停用之程序 55
4.9.16 憑證停用期間之限制 55
4.10 憑證狀態服務 55
4.10.1 操作特性 55
4.10.2 服務可用性 55
4.10.3 可選功能 56
4.11 訂購終止 56
4.12 私密金鑰託管及回復 56
4.12.1 金鑰託管及回復之政策及實務 56
4.12.2 會議金鑰封裝及回復之政策及實務 56
5 憑證機構設施、管理及操作控管 57
5.1 實體控管 57
5.1.1 所在位置與及結構 57
5.1.2 實體存取 57
5.1.3 電力及空調 58
5.1.4 水災防範 58
5.1.5 火災防範及保護 58
5.1.6 媒體儲存 58
5.1.7 廢料處理 58
5.1.8 異地備援 59
5.2 程序控管 59
5.2.1 信賴角色 59
5.2.2 每項任務所需之人數 61
5.2.3 識別及鑑別每個角色 63
5.2.4 需要職責分離之角色 64
5.3 人員控管 64
5.3.1 資格、經驗及清白規定 64
5.3.2 背景調查程序 65
5.3.3 教育訓練規定 65

5.3.4 人員再教育訓練之頻率及規定 66
5.3.5 工作輪調之頻率及順序 66
5.3.6 未授權行為之裁罰 67
5.3.7 承攬商派駐人員之規定 67
5.3.8 提供之文件 67
5.4 稽核紀錄程序 67
5.4.1 被記錄事件種類 68
5.4.2 紀錄檔處理頻率 71
5.4.3 稽核紀錄檔保留期限 71
5.4.4 稽核紀錄檔之保護 71
5.4.5 稽核紀錄檔備份程序 72
5.4.6 稽核彙整系統 72
5.4.7 對引起事件者之通知 72
5.4.8 弱點評估 72
5.5 紀錄歸檔 73
5.5.1 歸檔紀錄之種類 73
5.5.2 歸檔資料保留期限 73
5.5.3 歸檔資料之保護 74
5.5.4 歸檔資料備份程序 74
5.5.5 記錄之時戳規定 74
5.5.6 歸檔資料彙整系統 74
5.5.7 取得及驗證歸檔資料之程序 75
5.6 HiPKI RCA 之金鑰更換 75
5.7 破解及災變之復原 75
5.7.1 緊急事件及系統遭破解之處理程序 75
5.7.2 電腦資源、軟體或資料遭破壞 75
5.7.3 HiPKI RCA 私密金鑰遭破解之處理程序 76
5.7.4 災變後業務持續營運能力 76
5.8 HiPKI RCA 之終止服務 76
6 技術性安全控管 77
6.1 金鑰對之產製及安裝 77
6.1.1 金鑰對之產製 77
6.1.2 私密金鑰傳送給憑證機構 78
6.1.3 公開金鑰傳送給簽發憑證機構 78

6.1.4 憑證機構公開金鑰傳送給信賴憑證者 78
6.1.5 金鑰長度 79
6.1.6 公開金鑰參數之產製及品質檢驗 80
6.1.7 金鑰之使用目的 80
6.2 私密金鑰保護及密碼模組工程控管 81
6.2.1 密碼模組標準及控管 81
6.2.2 私密金鑰分持之多人控管 82
6.2.3 私密金鑰託管 82
6.2.4 私密金鑰備份 82
6.2.5 私密金鑰歸檔 83
6.2.6 私密金鑰匯入、匯出密碼模組 83
6.2.7 私密金鑰儲存於密碼模組 83
6.2.8 啟動私密金鑰之方式 83
6.2.9 停用私密金鑰之方式 84
6.2.10 銷毀私密金鑰之方式 84
6.2.11 密碼模組評等 85
6.3 金鑰對管理之其他規範 85
6.3.1 公開金鑰歸檔 85
6.3.2 憑證操作及金鑰對之使用期限 85
6.4 啟動資料 87
6.4.1 啟動資料之產生及安裝 87
6.4.2 啟動資料之保護 87
6.4.3 啟動資料之其他規範 88
6.5 電腦安全控管 88
6.5.1 特定電腦安全技術規定 88
6.5.2 電腦安全評等 88
6.6 生命週期技術控管 89
6.6.1 系統研發控管 89
6.6.2 安全管理控管 89
6.6.3 生命週期安全控管 89
6.7 網路安全控管 90
6.8 時戳 90
7 憑證、憑證廢止清冊及線上憑證狀態協定之格式剖繪 91
7.1 憑證之格式剖繪 91

7.1.1 版本序號 91
7.1.2 憑證擴充欄位 91
7.1.3 演算法物件識別碼 95
7.1.4 命名形式 96
7.1.5 命名限制 97
7.1.6 憑證政策物件識別碼 98
7.1.7 政策限制擴充欄位之使用 98
7.1.8 政策限定元之語法及語意 98
7.1.9 關鍵憑證政策擴充欄位之語意處理 98
7.2 憑證廢止清冊之格式剖繪 98
7.2.1 版本序號 98
7.2.2 憑證機構廢止清冊及憑證機構廢止清冊條目之擴充欄位 99
7.3 線上憑證狀態協定之格式剖繪 99
7.3.1 版本序號 99
7.3.2 線上憑證狀態協定擴充欄位 100
8 稽核及其他評核 101
8.1 稽核頻率或評核事項 101
8.2 稽核人員之身分及資格 101
8.3 稽核人員及被稽核方之關係 101
8.4 稽核項目 101
8.5 對於稽核結果之因應方式 102
8.6 稽核結果之公開 102
9 其他業務及法律事項 103
9.1 費用 103
9.1.1 憑證簽發、展期費用 103
9.1.2 憑證查詢費用 103
9.1.3 憑證廢止、狀態查詢費用 103
9.1.4 其他服務費用 103
9.1.5 退費 103
9.2 財務責任 103
9.2.1 保險涵蓋範圍 103
9.2.2 其他資產 104

9.2.3 對終端個體之保險或保固 104
9.3 業務資訊之保密 104
9.3.1 機密資訊之範圍 104
9.3.2 非機密之資訊 105
9.3.3 保護機密資訊之責任 105
9.4 個人資訊之隱私 105
9.4.1 隱私保護計畫 105
9.4.2 視為隱私之資訊 105
9.4.3 非隱私之資訊 106
9.4.4 保護隱私資訊之責任 106
9.4.5 使用隱私資訊之告知及同意 106
9.4.6 應司法或管理程序釋出資訊 106
9.4.7 其他資訊釋出之情況 106
9.5 智慧財產權 107
9.6 聲明及擔保 107
9.6.1 HiPKI RCA 之聲明及擔保 107
9.6.2 註冊中心之聲明及擔保 109
9.6.3 下屬憑證機構及交互認證憑證機構之聲明及擔保 109
9.6.4 信賴憑證者之聲明及擔保 111
9.6.5 其他參與者之聲明及擔保 112
9.7 免責聲明 112
9.8 責任限制 113
9.9 賠償 113
9.9.1 HiPKI RCA 之賠償責任 113
9.9.2 下屬憑證機構及交互認證機構之賠償責任 114
9.10 有效期限及終止 114
9.10.1 有效期限 114
9.10.2 終止 114
9.10.3 效力之終止及保留 115
9.11 主要成員之個別告知及溝通 115
9.12 修訂 115
9.12.1 修訂程序 115
9.12.2 通知之機制及期限 115
9.12.3 物件識別碼必須更改之情況 116

9.13 爭議解決條款.....116
9.14 管轄法律.....116
9.15 適用法律.....116
9.16 雜項條款.....116
9.16.1 完整協議.....116
9.16.2 轉讓.....117
9.16.3 可分割性.....117
9.16.4 契約履行.....117
9.16.5 不可抗力.....118
9.17 其他條款.....118

文件修訂歷程

版次	發行日期	修訂摘要
1.0	2019 年 2 月 22 日	首次發行。
1.05	2020 年 3 月 2 日	(1) 依據 Baseline Requirements 第 1.6.7 版及營運現況修訂第 1.5.2、第 3.2.5、第 4.9、第 6.2.6 及第 9.6 節，並增加第 3.2.7 節。 (2) 依據 RFC 3647 與營運現況，修訂第 5.3.7 節「約聘人員」用詞為「承攬商派駐人員」，並修訂安全規定。 (3) 依據 Mozilla Root Store Policy 2.7 版，修訂第 7.1.2、第 7.1.5 及第 7.1.8 節關於延伸金鑰用途欄位及憑證政策擴充欄位之描述。 (4) 修訂第 1.6、第 6.1.7、第 6.3.2、第 7.1.3、第 7.2.2、第 7.3.1 及第 9.6.3.2 節。
1.1	2020 年 7 月 2 日	(1) 經濟部核定版本(涵蓋中華電信憑證政策管理委員會通過之第 1.0 與第 1.05 版) (2) 修訂第 1.3.3、第 1.3.4、第 1.4.2、第 1.5.4、第 1.6.1 及第 4.2.1.1 節

摘要

HiPKI 憑證總管理中心憑證實務作業基準之重要事項說明如下：(依據電子簽章法第 11 條及經濟部頒訂之『憑證實務作業基準應載明事項準則』之規定)

1、主管機關核定文號：經商字第 10900635970 號

2、簽發之憑證：

(1) 種類：HiPKI 憑證總管理中心(簡稱總管理中心或 HiPKI RCA)之自簽憑證、自發憑證、簽發給下屬憑證機構(Subordinate CA)之下屬憑證機構憑證(Subordinate CA Certificate)與簽發給交互認證憑證機構之交互憑證。

(2) 保證等級：依據 HiPKI 憑證政策，於組織憑證及個人憑證簽發 4 種保證等級的憑證，TLS/SSL 憑證或 Code Signing 憑證則依照憑證機構與瀏覽器論壇(CA/Browser Forum)所定義的保證等級。

(3) 適用範圍：

自簽憑證之簽發對象為HiPKI RCA本身，內含HiPKI RCA的公開金鑰，可用來驗證HiPKI RCA簽發之下屬憑證機構憑證、交互憑證、自發憑證與憑證機構廢止清冊的數位簽章。

自發憑證為HiPKI RCA更換金鑰或憑證政策所簽發之憑證，用以建立新舊金鑰間或憑證政策互通信賴路徑之用。

下屬憑證機構憑證之簽發對象為HiPKI之下屬憑證機構。下屬憑證機構憑證內含下屬憑證機構的公開金鑰，可用來驗證下屬憑證機構所簽發之憑證與憑證廢止清冊的數位簽章。

交互憑證之簽發對象為與HiPKI RCA進行交互認證之另一公開金鑰基礎建設的根憑證機構(Root Certification Authority, Root CA)，亦即此憑證機構為HiPKI外之憑證機構。交互憑證內含交互認證憑證機構的公開金鑰，可用來驗證該憑證機構簽發之憑證與憑證機構廢止清冊的數位簽章。

3、法律責任重要事項：

(1) 下屬憑證機構、交互認證憑證機構或信賴憑證者(Relying Party)如未依照憑證實務作業基準規定之適用範圍使用憑證所引發之後果，HiPKI RCA 不負任何法律責任。

(2) 與 HiPKI RCA 交互認證之憑證機構，因簽發憑證或使用憑證而發生損害賠償事件時，HiPKI RCA 之損害賠償責

任以本作業基準及與各該交互認證機構簽訂之契約所訂定之責任範圍為限。

(3) 如因不可抗力及其他非可歸責於 HiPKI RCA 之事由，所導致之損害事件，HiPKI RCA 不負任何法律責任。

(4) 如因 HiPKI RCA 之系統維護、轉換及擴充等需要，得暫停部分憑證服務，並公告於儲存庫及通知憑證機構，信賴憑證者、下屬憑證機構或交互認證憑證機構不得以此作為要求 HiPKI RCA 損害賠償之理由。

4、其他重要事項：

(1) HiPKI RCA 直接受理憑證註冊與廢止申請等工作，因此不另設立註冊中心(Registration Authority, RA)。

(2) HiPKI RCA 簽發之憑證，依不同保證等級有不同之適用範圍，下屬憑證機構或交互認證憑證機構於提出下屬憑證機構憑證申請或交互認證申請時，必須敘明所申請憑證之保證等級。

(3) 申請下屬憑證機構憑證或交互認證之憑證機構必須自行產製私密金鑰，並妥善保管及使用。

(4) 在憑證機構接受 HiPKI RCA 所簽發之憑證後，即表示該憑證機構已確認憑證內容資訊之正確性。

(5) 下屬憑證機構或交互認證憑證機構如有廢止憑證之必要時，應儘速通知 HiPKI RCA，並應遵守憑證實務作業基準規定程序辦理，但下屬憑證機構或交互認證憑證機構於憑證廢止狀態未被公布之前，應先行採取適當的行動，以減少對下屬憑證機構或交互認證憑證機構或信賴憑證者之影響，並承擔所有因使用該憑證所引發之法律責任。

(6) 信賴憑證者在使用 HiPKI RCA 簽發之憑證時，應先確認該憑證之正確性、有效性、保證等級及用途限制。

(7) 中華電信股份有限公司(簡稱本公司)將委託公正之第三方，就 HiPKI RCA 與下屬憑證管理中心的運作採用 WebTrust Principles and Criteria for Certification Authorities(簡稱 WebTrust for CA)、WebTrust Principles and Criteria for Certification Authorities－SSL Baseline with Network Security(簡稱 WebTrust for CA－SSL BR)與 WebTrust Principles and Criteria for Certification Authorities－Extended Validation SSL (簡稱 WebTrust for CA－EV SSL)進行稽核。

1 序論

1.1 概要

1.1.1 憑證實務作業基準

HiPKI 憑證總管理中心(HiPKI Root Certification Authority，簡稱 HiPKI RCA)憑證實務作業基準(Certification Practice Statement，簡稱本作業基準)係依據 HiPKI 憑證政策(HiPKI Certificate Policy)所訂定，並遵循

(1) 電子簽章法

(2) 及其子法「憑證實務作業基準應載明事項準則」

之相關規定及國際相關標準如：

(1) 網際網路工程任務小組(Internet Engineering Task Force, IETF) 徵求修正意見書(Request for Comments, RFC) 3647 與 RFC 5280

(2) ITU-T X.509

(3) 憑證機構與瀏覽器論壇(CA/Browser Forum, http://www.cabforum.org)發行之最新版 Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates(簡稱 Baseline Requirements)、Guidelines for the Issuance and Management of Extended Validation Certificates(簡稱 EV SSL Certificate Guidelines)、Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates(簡稱 EV Code Signing Guidelines)及 Network and Certificate System Security Requirements

(4) Minimum Requirements for the Issuance and Management of

Publicly-Trusted Code Signing Certificates(簡稱 Code Signing BR)

所訂定之憑證實務作業文件，以做為 HiPKI RCA 之下屬憑證機構(Subordinate CA)訂定憑證實務作業基準之依循。

本作業基準主要說明 HiPKI RCA 如何遵照 HiPKI 憑證政策保證等級(Assurance Level)第 4 級的規定，進行自簽憑證(Self-Signed Certificate)、自發憑證(Self-Issued Certificate)、下屬憑證機構憑證及交互憑證(Cross-Certificate)的簽發及管理作業。

依據 HiPKI 憑證政策的規定，HiPKI RCA 是 HiPKI (簡稱本基礎建設)的最頂層憑證機構，也是本基礎建設的信賴起源(Trust Anchor)，具備最高的公信度，信賴憑證者(Relying Party)可直接信賴 HiPKI RCA 本身的憑證。

SSL(Secure Sockets Layer)協定已由 TLS(Transport Layer Security)協定取代，因 SSL 憑證與 TLS 憑證指的是同樣可以讓 TLS 協定運作的憑證，而且漸漸有以 TLS 憑證取代廣泛使用的 SSL 憑證稱呼，為避免混淆，本作業基準多數地方會以 TLS/SSL 憑證表示。

依照 ITU-T X.509 標準，憑證政策所定義的保證等級必須以憑證政策物件識別碼(Object Identifier, OID，詳見第 1.2 節)表示，而這些憑證政策物件識別碼將會記載在憑證的憑證政策擴充欄位(Certificate Policies Extension)中。

保證等級係指信賴憑證者對於以下項目的信任程度：

(1) 憑證機構簽發之憑證，可分為兩種情形，如簽發憑證給終端個體(End Entities, EE)時，憑證政策物件識別碼代表該憑證申請時是依何種保證等級來做身分鑑別及簽發；如簽發憑證給

憑證機構時，則該憑證機構的憑證中可能會有 1 個以上的憑證政策物件識別碼，表示該憑證機構可以簽發符合憑證政策物件識別碼之保證等級的憑證給終端個體。

(2) 憑證之簽發與管理以及私密金鑰(Private Key)之傳送等憑證機構相關作業程序。

(3) 憑證中的用戶(Subscriber)或主體(Subject)是否能有效控管其憑證中所記載的公開金鑰成配對關係之私密金鑰，例如用戶使用軟體或硬體儲存其私密金鑰；亦即信賴憑證者能否確信憑證中所記載的主體與公開金鑰(Public Key)之連結關係(Binding)。

本基礎建設之憑證機構於簽發憑證時應引用適合的憑證政策物件識別碼，透過成對的憑證政策物件識別碼可確認簽發憑證機構(Issuing CA)與主體憑證機構(Subject CA)之間的憑證政策對應關係。

1.1.2 憑證實務作業基準之適用範圍

本作業基準所載明之實務作業規範適用於與 HiPKI RCA 相關之個體，包括 HiPKI RCA、下屬憑證機構、交互認證憑證機構(Cross-certified CA)及信賴憑證者等。

本作業基準並未授權 HiPKI RCA 以外的憑證機構使用，其他憑證機構因引用本作業基準而引發的任何問題，概由該憑證機構自行負責。

1.2 文件名稱及識別

本文件的名稱為 HiPKI 憑證總管理中心憑證實務作業基準(HiPKI RCA Certificate Practice Statement)，核定日期為 109 年 7 月 2

日，本作業基準之最新版本可在以下網頁取得：https://eca.hinet.net。本基礎建設之憑證機構可簽發的憑證列表如下：

(1) 個人(Individual)憑證

(2) 組織(Organization)憑證

(3) 網域驗證(Domain Validation, DV)型 TLS/SSL 憑證

(4) 組織驗證(Organization Validation, OV)型 TLS/SSL 憑證

(5) 個人驗證(Individual Validation, IV)型 TLS/SSL 憑證

(6) 延伸驗證(Extended Validation, EV)型 TLS/SSL 憑證

(7) 延伸驗證型程式碼簽章(EV Code Signing)憑證

(8) 一般驗證型程式碼簽章(Code Signing)憑證

(9) 時戳(Time-stamping)憑證

對於個人憑證及組織憑證，本基礎建設依照鑑別方式及適用範圍的不同，將其分成 4 個保證等級。保證等級越高，安全等級及可信賴度越高，且鑑別方式越嚴格。

憑證機構簽發的憑證(不含自簽憑證)必須在憑證政策擴充欄位記載憑證的憑證政策。下表為本基礎建設對 HiPKI 憑證政策及憑證機構之憑證實務作業基準提到的各類憑證及文件所設定之物件識別碼參照表：

物件名稱	物件識別碼
憑證政策	1 3 6 1 4 1 23459 200 0
保證等級	
第 1 級	1 3 6 1 4 1 23459 200 0 1
第 2 級	1 3 6 1 4 1 23459 200 0 2

物件名稱	物件識別碼
第 3 級	1 3 6 1 4 1 23459 200 0 3
第 4 級	1 3 6 1 4 1 23459 200 0 4
Baseline Requirements	
網域驗證型 TLS/SSL 憑證	2.23.140.1.2.1
組織驗證型 TLS/SSL 憑證	2.23.140.1.2.2
個人驗證型 TLS/SSL 憑證	2.23.140.1.2.3
EV SSL Certificate Guidelines	
延伸驗證型 TLS/SSL 憑證	2.23.140.1.1 (EV SSL Certificate Guidelines)
延伸驗證型程式碼簽章憑證	2.23.140.1.3
一般驗證型程式碼簽章憑證	2.23.140.1.4.1

其中以{2.23.140}為開頭的物件識別碼係參照憑證機構與瀏覽器論壇依據不同文件及憑證使用範圍所定義；而 arc 值 id-pen-cht ::= {1 3 6 1 4 1 23459}是中華電信股份有限公司(簡稱本公司)在網際網路號碼分配機構(Internet Assigned Numbers Authority, IANA)註冊之私人企業號碼(Private Enterprise Number, PEN)，本基礎建設使用的物件識別碼是{1 3 6 1 4 1 23459 200}，並依照不同憑證簽發保證等級分配不同物件識別碼進行區別。

下屬憑證機構其延伸驗證型 TLS/SSL 憑證簽發若符合 EV SSL Certificate Guidelines 之規定，並和應用軟體供應商(Application Software Suppliers，如瀏覽器或作業系統廠商)個別商議其所支援之憑證處置方式，下屬憑證機構的憑證及用戶之 TLS/SSL 憑證可使用憑證機構與瀏覽器論壇之延伸驗證型 TLS/SSL 憑證物件識別碼({joint

– iso – itu – t(2) international – organizations(23) ca – browser – forum(140) certificate– policies(1) ev-guidelines (1) }(2.23.140.1.1))。

若有任何本作業基準在 TLS/SSL 憑證簽發上與 Baseline Requirements 之規定有任何不一致的情形，將優先遵循 Baseline Requirements 的條款;若有任何本作業基準在延伸驗證型 TLS/SSL 憑證簽發上與 EV SSL Certificate Guidelines 之規定有任何不一致的情形，將優先遵循 EV SSL Certificate Guidelines 的條款。

1.3 主要成員

本憑證機構之主要成員包括：

(1) HiPKI RCA

(2) 下屬憑證機構

(3) 交互認證憑證機構

(4) 信賴憑證者

1.3.1 憑證機構

1.3.1.1 HiPKI RCA

HiPKI RCA 為本基礎建設的根憑證機構(Root Certification Authority, Root CA)，也是代表本基礎建設的主要憑證機構(Principal CA)。HiPKI RCA 由本公司負責建置及營運，主要工作說明如下：

(1) 負責 HiPKI RCA 之自簽憑證、自發憑證與下屬憑證機構憑證之簽發及管理。

(2) 訂定與本基礎建設外之根憑證機構間的交互認證程序，包括簽發及管理其他本基礎建設外根憑證機構的交互憑證。

(3)將簽發的憑證機構廢止清冊(Certification Authority Revocation List, CARL，詳見第 1.6.1 節)公布於儲存庫(Repository)，並且確保儲存庫之正常運作。

1.3.1.2 下屬憑證機構

下屬憑證機構為本基礎建設中的另一種憑證機構，主要負責簽發及管理終端個體的憑證，必要時也可依階層式公開金鑰基礎建設的建構方式，由第 1 層下屬憑證機構簽發憑證給第 2 層下屬憑證機構，或由第 2 層下屬憑證機構簽發憑證給第 3 層下屬憑證機構，依此類推而建構 1 個多層次的 PKI。但下屬憑證機構不可以直接與本基礎建設外的憑證機構進行交互認證。

下屬憑證機構之建置應依照憑證政策相關規定，並設置聯絡窗口，負責與 HiPKI RCA 及其他下屬憑證機構之互運工作。

本基礎建設的第 1 層下屬憑證機構包含 HiPKI EV TLS 憑證管理中心，由本公司負責營運。

1.3.1.3 交互認證憑證機構

交互認證憑證機構係指與 HiPKI RCA 進行交互認證之憑證機構，為本基礎建設外之根憑證機構。欲向 HiPKI RCA 申請交互認證之根憑證機構，必須符合所引用的憑證政策保證等級之安全性規定，具備公開金鑰基礎建設及數位簽章及憑證簽發技術之建置及管理能力，訂定憑證機構、註冊中心及信賴憑證者之相關責任及義務，並通過與本基礎建設相同強度的憑證機構外部稽核。

1.3.2 註冊中心

HiPKI RCA 直接受理憑證註冊與廢止申請等工作，負責蒐集及驗證下屬憑證機構、交互認證憑證機構之身分及憑證相關資訊，不另設立註冊中心。

1.3.3 用戶

用戶係指不具備憑證簽發能力之憑證主體，並擁有與憑證記載之公開金鑰相對應之私密金鑰的個體。在憑證政策及本作業基準中並不稱根憑證機構、下屬憑證機構或交互認證憑證管理中心為用戶，因其具有憑證簽發之能力。

1.3.4 信賴憑證者

信賴憑證者係指相信憑證主體名稱與某公開金鑰間連結關係的個體。信賴憑證者必須依照相對的憑證機構憑證及憑證狀態資訊，以驗證所收到憑證的有效性。在確認憑證的有效性後，才可使用憑證進行以下作業：

(1) 驗證具有數位簽章的電子文件之完整性

(2) 驗證電子文件簽章產生者的身分

(3) 與憑證主體間建立安全之通訊管道

1.3.5 其他相關成員

若 HiPKI RCA 有選擇其他相關提供信賴服務機構做為協同運作的夥伴，例如橋接式憑證管理中心、時戳服務機構(Time Stamping Authority)、資料存證服務機構(Data Archiving Service Authority)等，會於網站揭露並於本作業基準中訂定相互運作機制及彼此的權利與義務關係，以確保本管理中心服務品質的有效及可靠。

1.4 憑證用途

1.4.1 憑證之適用範圍

HiPKI RCA 簽發的憑證有 4 種，分別為自簽憑證、自發憑證、下屬憑證機構憑證與交互憑證。

自簽憑證用以建立 HiPKI 信賴的起源。自發憑證為 HiPKI RCA 更換金鑰或憑證政策互通信賴路徑之用。下屬憑證機構憑證用以建立同一公開金鑰基礎建設之憑證機構間的互相信賴關係，以建構憑證機構互通所需的憑證信賴路徑之用。交互憑證用以建立不同公開金鑰基礎建設之根憑證機構間的互相信賴關係，以建構憑證機構互通所需的憑證信賴路徑之用。

自簽憑證之簽發對象為 HiPKI RCA 本身，內含 HiPKI RCA 的公開金鑰，可用來驗證 HiPKI RCA 簽發之下屬憑證機構憑證、交互憑證、自發憑證與憑證機構廢止清冊的數位簽章。

下屬憑證機構憑證之簽發對象為 HiPKI 之下屬憑證機構。下屬憑證機構憑證內含下屬憑證機構的公開金鑰，可用來驗證下屬憑證機構所簽發之憑證與憑證廢止清冊的數位簽章。

交互憑證之簽發對象為與 HiPKI RCA 進行交互認證之本基礎建設外之公開金鑰基礎建設的根憑證機構。交互憑證內含交互認證憑證機構的公開金鑰，可用來驗證該根憑證機構簽發之憑證與憑證機構廢止清冊的數位簽章。

信賴憑證者應依照第 6.1.4 節所述之自簽憑證安全散布管道取得所信賴的 HiPKI RCA 之公開金鑰或自簽憑證，始可用以驗證 HiPKI RCA 簽發之自發憑證、下屬憑證機構憑證、交互憑證與憑證機構廢止清冊的數位簽章。

信賴憑證者應慎選安全的電腦環境及可信賴的應用系統，避免所取得儲存的 HiPKI RCA 之公開金鑰或自簽憑證遭破壞或更換，俾可確保使用正確的 HiPKI RCA 公開金鑰或自簽憑證來驗證 HiPKI RCA 簽發之自發憑證、下屬憑證機構憑證、交互憑證與憑證機構廢止清冊的數位簽章。

HiPKI RCA 簽發給下屬憑證機構的憑證中，將記載該下屬憑證機構可以簽發何種保證等級之憑證，以供信賴憑證者決定是否信賴該下屬憑證機構及其所簽發的憑證。

HiPKI RCA 簽發給本基礎建設外的根憑證機構的交互憑證中，將記載該憑證機構可以簽發何種保證等級之憑證及可再與其他根憑證機構進行交互認證之層數，另外，交互憑證中也會包括該根憑證機構所採用的憑證政策對應(Policy Mapping)關係，以供信賴憑證者決定是否信賴該憑證機構及其所簽發的憑證。

信賴憑證者必須依照第 6.1.7 節金鑰之使用目的之規定，適當地使用金鑰，並使用符合國際標準(例如 ITU-T X.509 標準或 RFC 5280 等)定義之憑證驗證(certificate validation)方法來驗證憑證的有效性(validity)。

信賴憑證者在使用 HiPKI RCA 所提供的認證服務前，必須詳細閱讀本作業基準，並遵守本作業基準之規定，同時必須注意本作業基準之更新。

1.4.2 憑證之禁用範圍

本管理中心所簽發的憑證禁止使用於下列的情況：

(1) 犯罪

(2) 軍令戰情及核生化武器管制

(3)核能運轉設備

(4)航空飛行及管制系統

1.5 政策管理

1.5.1 憑證實務作業基準之管理機構

中華電信股份有限公司。

1.5.2 聯絡資料

1.5.2.1 憑證實務作業基準建議

對本作業基準有疑義需要諮詢，或有修訂建議，請利用以下資訊與 HiPKI RCA 聯絡：

聯絡電話：886 2-2344-4820

郵遞地址：10048 台北市信義路一段 21 號數據通信大樓 4F

HiPKI 憑證總管理中心

電子郵件信箱：caservice@cht.com.tw。

也可至https://eca.hinet.net查詢聯絡資料。

1.5.2.2 憑證問題報告

憑證機構、信賴憑證者、應用軟體供應商以及其他第三方組織於發現私密金鑰遺失、疑似私密金鑰遭破解、憑證遭誤用、或是憑證被偽造、破解、濫用等情況時(包含工作日以外時間)，可寄送電子郵件至 report_abuse@cht.com.tw 向 HiPKI RCA 提出憑證問題報告(Certificate Problem Report)。

相關說明請參見第 4.9.3.3 及第 4.9.5 節，由 HiPKI RCA 決定是否廢止該憑證。

1.5.3 憑證實務作業基準之審定

HiPKI RCA 於檢查本作業基準是否符合本基礎建設的憑證政策相關規定後，送中華電信憑證政策管理委員會(簡稱政策管理委員會)進行審查及核定。

另依據我國電子簽章法規定，憑證機構訂定之憑證實務作業基準，必須經主管機關經濟部核定後，始得對外提供簽發憑證服務。

HiPKI RCA 定期自行稽核，以證明遵照引用於憑證政策之保證等級進行營運。為使本基礎建設所發之憑證順暢運作於各作業系統、瀏覽器與軟體平台，本基礎建設已經申請參與各作業系統、瀏覽器與軟體平台之根憑證計畫(Root Certificate Program)，將 HiPKI RCA 之自簽憑證廣泛部署於各軟體平台之憑證機構信賴清單(CA Trust List)。

依據根憑證計畫之規定，採連續不中斷涵蓋整個公開金鑰基礎建設之原則，每年併同各下屬憑證機構執行外部稽核並將最新之憑證實務作業基準與外部稽核的結果提供給各大根憑證計畫，並持續維護稽核標章公告於 HiPKI RCA 網站。

1.5.4 憑證實務作業基準之核准程序

本作業基準經政策管理委員會或電子簽章法主管機關經濟部核定後，由 HiPKI RCA 公布。如憑證政策的修訂公告後，本作業基準將配合修訂，先送政策管理委員會審查後，再送交電子簽章法主管機關經濟部核定。

本作業基準修訂生效後，除另有規定外，如修訂之版本與原本作業基準有所牴觸時，以修訂之版本為準。

1.6 名詞定義及縮寫

1.6.1 名詞定義

中/英文名詞	定義
存取(Access)	運用系統資源處理資訊的能力。
存取控制 (Access Control)	對於授權的使用者、程式、程序或其他系統給予資訊系統資源存取權限的處理過程。
啟動資料 (Activation Data)	在存取密碼模組時(例如用來開啟私密金鑰以進行簽章或解密)，除金鑰外所需及應受保護之隱密資料。
申請者 (Applicant)	向憑證機構申請憑證，而尚未完成憑證簽發作業程序的用戶。
歸檔 (Archive)	實體上(與主要資料存放處)分隔的長期資料儲存處，可用來支援稽核服務、可用性服務或完整性服務等用途。
保證 (Assurance)	據以信賴該個體已符合特定安全要件之基礎。[憑證實務作業基準應載明事項準則第 2 條第 1 款]
保證等級 (Assurance Level)	具相對性保證層級中之某 1 級數。[憑證實務作業基準應載明事項準則第 2 條第 2 款]
稽核 (Audit)	評估系統控制的是否恰當、確保符合既定的政策及營運程序、並對現有的控制、政策及程序建議必要的改善而進行的獨立檢閱及調查。
稽核紀錄 (Audit Data)	依照發生時間順序之系統活動紀錄，可用以重建或調查事件發生的順序及某個事件中的變化。
鑑別(Authenticate)	當某個體出示身分時，確認其身分之正確性。
鑑別程序 (Authentication)	(1)建立使用者到資訊系統身分信賴程度的程序。[NIST.SP.800-63-2 Electronic Authentication Guideline] (2)用以建立資料傳送之安全措施，或是驗證

中/英文名詞	定義
	個人接收特定種類資訊權限之方法。 (3)鑑別是身分的證明程序。[A Guide to Understanding Identification and Authentication in Trusted Systems] 而所謂的相互鑑別(Mutual Authentication)是指在進行通訊活動的兩方彼此進行鑑別。
憑證機構資訊存取 (Authority Information Access, AIA)	記載有關存取憑證機構資訊的擴充欄位，內容可包含：線上憑證狀態協定的服務位址，以及簽發憑證機構之憑證驗證路徑的下載位址等。
備份(Backup)	將資料或程式複製，必要時可供復原之用。
連結、繫結(Binding)	將兩個相關的資訊元素做連結(結合)的過程。
生物特徵值(Biometric)	人的身體或行為的特徵。
憑證機構憑證 (CA Certificate)	簽發給憑證機構的憑證。
能力成熟度模型整合 (Capability Maturity Model Integration, CMMI)	由美國卡內基美隆大學(Carnegie Mellon University)的軟體工程研究所(Software Engineering Institute)自CMM之後提出的修訂版本。CMMI 模型能為開發或改進用於達成一個組織的商業目標的過程提供指導，其目的是協助提升組織的績效。
憑證 (Certificate)	(1)指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。[電子簽章法第2條第6款] (2)資訊之數位呈現，內容至少包括： a. 簽發的憑證機構 b. 用戶之名稱或身分 c. 用戶的公開金鑰 d. 憑證之有效期間 e. 簽發憑證機構之數位簽章 在本憑證政策中所提及的“憑證”特別指其

中/英文名詞	定義
	格式為 X.509 v3，且在其“憑證政策”欄位中明確地引用本憑證政策之物件識別碼的憑證。
憑證機構(Certification Authority, CA)	(1)簽發憑證之機關、法人。[電子簽章法第 2 條第 5 款] (2)為使用者所信任之權威機構，其業務為簽發並管理 ITU-T X.509 格式之公開金鑰憑證及憑證廢止清冊(或憑證機構廢止清冊)。
憑證機構廢止清冊 (Certification Authority Revocation List, CARL)	可供信賴憑證者查詢用之已廢止憑證清單，該清單中記載在到期日前被廢止之憑證機構憑證(包括自發憑證、下屬憑證機構憑證或交互憑證)及廢止時間與原因等資訊，由簽發憑證之根憑證機構以數位簽章的方式確保其完整性與不可否認性。
憑證政策 (Certificate Policy, CP)	(1)某 1 憑證所適用之對象或情況所列舉之 1 套規則，該對象或情況可為特定之社群或具共同安全需求之應用。[憑證實務作業基準應載明事項準則第 2 條第 3 款] (2)憑證政策係為透過憑證管理執行的電子交易所訂定之具專門格式的管理政策。憑證政策中包括與數位憑證相關之生成、產製、傳送、稽核、被破解後的復原以及其管理等各項議題。憑證政策亦可間接地控制運用憑證之安全系統，以保護通訊系統所進行的交易。藉由控制關鍵的憑證擴充欄位方式，憑證政策及其相關技術可提供特定應用所需的安全服務。
憑證實務作業基準 (Certification Practice Statement, CPS)	(1)由憑證機構對外公告，用以陳述憑證機構據以簽發憑證及處理其他認證業務之作業準則。[電子簽章法第 2 條第 7 款] (2)宣告某憑證機構對憑證之作業程序(包括簽發、停用、廢止、展期及金鑰更換等)符合特定需求(需求載明於憑證政策或其他

中/英文名詞	定義
	服務契約中)之聲明。
憑證金鑰更換 (Certificate Re-key)	改變在密碼系統應用程式中所使用之金鑰對。通常必須藉由對新的公開金鑰簽發新的憑證來達成新的金鑰對替換的目的。
憑證展期 (Certificate Renewal)	藉由簽發新的憑證，以延展原憑證內所連結資料有效性的程序。
憑證廢止 (Certificate Revocation)	在憑證的有效期間內，提前終止憑證的運作。
憑證問題報告 (Certificate Problem Report)	疑似金鑰遭破解、憑證遭誤用(misuse)或其他種類的詐騙、破解、濫用或與憑證相關的不當行為之投訴。
憑證廢止清冊 (Certificate Revocation List, CRL)	由憑證機構以數位方式簽署且會定期更新之已廢止憑證清冊，清冊中記載由此憑證機構所簽發且在到期日之前被廢止之憑證。
憑證透明化(Certificate Transparency, CT)	憑證透明化機制為一個公開監控與稽核網際網路上所有憑證的開放性架構(現階段以 TLS/SSL 憑證為優先目標)，透過公開憑證的簽發與存在等資訊給網域所有者、憑證機構、以及網域使用者，供其判斷憑證是否被錯誤或惡意簽發；換言之，其目的係提供一個可用於監控 TLS/SSL 憑證機制與審核特定 TLS/SSL 憑證的公開監控與資訊公開的環境，以遏止憑證相關威脅。憑證透明化機制，主要由憑證日誌、憑證監控者、以及憑證稽核者等三個要素所組成。
中華電信憑證政策管理委員會(Chunghwa Telecom Certificate Policy Management Authority，簡稱政策管理委員會)	1 組織，其設立目的為：研議中華電信所經營之公開基礎建設其憑證政策及電子憑證體系架構、審核下屬憑證機構與交互證認證憑證機構的互運申請及其他如審議憑證實務作業基準等電子憑證管理事項。
破解 (Compromise)	資訊洩漏給未經授權的人士或違反資訊安全政策造成物件未經授權蓄意、非蓄意的洩

中/英文名詞	定義
	漏、修改、毀壞或遺失。
機密性 (Confidentiality)	資訊不會遭受未經授權的個體或程序獲知或取用。
交互憑證 (Cross-Certificate)	在兩個根憑證機構(Root CA)之間建立信賴關係的 1 種憑證，屬於 1 種憑證機構憑證，而非用戶憑證。
交互認證協議書 (Cross Certification Agreement, CCA)	根憑證機構與交互認證憑證機構就交互憑證機構申請加入該根憑證機構所在之公開金鑰基礎建設，所必須遵守之事項及個別責任義務歸屬的協議。
密碼模組 (Cryptographic Module)	1 組硬體、軟體、韌體或前述的組合，用以執行密碼的邏輯或程序(包含密碼演算法)，並且被包含在此模組的密碼邊界之內。
資料完整性 (Data Integrity)	保證資料從發文者產製完到被收文者接受都未遭竄改。
數位簽章 (Digital Signature)	將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。[電子簽章法第 2 條第 3 款]
網域名稱 (Domain Name)	在網域名稱系統分配給 1 個節點(node)的標籤(label)。亦即轉換 IP 位址為人類容易記憶之文字名稱。
網域名稱系統(Domain Name System, DNS)	將網域名稱轉換為 IP 位址的網路服務。
網域驗證 (Domain Validation, DV)	TLS/SSL 憑證核發過程中，只會驗證用戶之網域擁有權或控制權，但並未識別及鑑別用戶之組織或個人身分。故連結安裝網域驗證型 TLS/SSL 憑證之網站，可提供 TLS 加密通道，但無法知道該網站之擁有者是誰。
憑證效期 (Duration)	1 憑證欄位，由“有效期限起始時間”(notBefore) 及“有效期限截止時間”(notBefore)兩個子欄位所組成。

中/英文名詞	定義
電子商務 (E-commerce)	使用網路科技(特別是網際網路)以提供買賣貨物及相關服務。
終端個體憑證 (End-Entity Certificate)	簽發給終端個體的憑證。
延伸驗證型程式碼簽章憑證(EV Code Signing Certificate)	依據 EV Code Signing Guidelines 所簽發之憑證。
延伸驗證型 TLS/SSL 憑證(EV TLS/SSL Certificate)	依據 EV SSL Certificate Guidelines 之規定，憑證的主體欄位必須記載經過驗證的資訊。
延伸驗證(Extended Validation, EV)	EV SSL Certificate Guidelines 所定義之驗證程序。
聯邦資訊處理標準 (Federal Information Processing Standard, FIPS)	為美國聯邦政府制定除軍事機構外，所有政府機構及政府承包商所引用之資訊處理標準。其中密碼模組安全需求標準為 FIPS 第 140 號標準(簡稱 FIPS 140)，到 2016 年 12 月為止此標準的最新版本為 FIPS 140-2。FIPS 140 將密碼模組區分為 11 類需求範圍，而 FIPS 140-2 則定義了 4 個安全等級。
防火牆 (Firewall)	符合近端(區域)安全政策而對網路之間做接取限制的閘道器。
完全吻合網域名稱 (Fully Qualified Domain Name, FQDN)	1 種用於指定電腦在網域階層中確切位置的明確網域名稱。FQDN 包含主機名稱（服務名稱）與網域名稱兩部分。例如 ourserver.ourdomain.com.tw。ourserver 是主機名稱，ourdomain.com.tw 是網域名稱，其中 ourdomain 是第 3 層網域名稱，com 則是次級網域名稱(Second-Level Domain)，tw 則是國碼頂級網域名稱(Country Code Top-Level Domain, ccTLD)。FQDN 的開頭一定是主機名稱。
HiPKI	中華電信股份有限公司為推動電子化服務，依照 ITU-T X.509 標準建置的階層式公開金

中/英文名詞	定義
	鑰基礎建設。
HiPKI 憑證總管理中心 (HiPKI Root Certification Authority, HiPKI RCA)	HiPKI 的根憑證機構(Root CA)，在此階層式公開金鑰基礎建設架構中屬於最頂層的憑證機構，其公開金鑰為信賴之起源。
個人驗證(Individual Validation, IV)	TLS/SSL 憑證核發過程中，除了驗證用戶之網域擁有權或控制權外，並且依照憑證的保證等級識別及鑑別用戶之個人身分。故連結安裝個人驗證型 TLS/SSL 憑證之網站，可提供 TLS 加密通道，知道該網站之擁有者屬於哪一個自然人，並確保資料傳遞之完整性。
識別 (Identification)	識別是某使用者是誰(廣為週知)的陳述方式或表達方式。[A Guide to Understanding Identification and Authentication in Trusted Systems] 識別是指描述或宣稱某個當事人或個體的方式，例如透過使用者帳號、姓名或電子郵件。
完整性 (Integrity)	對資訊的保護，使其不受未經授權的修改或破壞。資訊從來源產製後，經傳送、儲存到最終被收受方接收的期間中都維持不被篡改的一種狀態。
網際網路號碼分配機構 (Internet Assigned Numbers Authority, IANA)	負責管理國際網際網路中使用的 IP 位址、網域名稱及許多其它參數之組織。
網際網路工程任務小組 (Internet Engineering Task Force, IETF)	負責網際網路標準的開發和推動之組織，包含網際網路架構及操作，使得網際網路運作更順暢，官方網站位於 https://www.ietf.org/。
簽發憑證機構 (Issuing CA)	對於 1 張憑證而言，簽發該憑證的憑證機構即稱為該憑證的簽發憑證機構。
金鑰破解 (Key Compromise)	私密金鑰被他人未經授權的使用或揭露。
金鑰託管	依據用戶必須遵守的託管協議(或類似的契

中/英文名詞	定義
(Key Escrow)	約)所規定，將用戶的私密金鑰進行存放。此託管協議的條款要求 1 個或 1 個以上的代理機構基於有益於用戶、雇主或另一方的前提下，擁有用戶加密用的私密金鑰。
金鑰對 (Key Pair)	兩把數學上有相關性的金鑰，具有下列特性： (1)其中 1 把金鑰用來做訊息加密，而此加密訊息只有用成對關係的另 1 把金鑰可以解密。 (2)從其中 1 把金鑰要推出另 1 把金鑰(從計算的角度而言)是不可行的。
(美國)國家標準和技術研究院(National Institute of Standards and Technology, NIST)	官方網站在http://www.nist.gov/，類似我國的經濟部國家標準檢驗局，其使命係促進美國的創新和產業競爭力，推動度量衡學、標準、技術以提高經濟安全並改善生活品質。其所制定之硬體密碼模組標準及驗證、金鑰安全評估報告或聯邦政府的公務員和承包商身分卡標準廣泛被參考或引用。
不可否認性 (Non-Repudiation)	公開金鑰密碼系統所提供的技術性證據以支援不可否認之安全服務。 對資料傳送方提供傳送證明以及對資料收受方提供傳送方的身分之保證，因而兩方在事後皆無法否認曾經處理過此項資料。技術上的不可否認性是指對信賴憑證者而言，如果某個公開金鑰可用以驗核某個數位簽章，保證此簽章必定是由相對應的私密金鑰所簽署。
物件識別碼(Object Identifier, OID)	(1)1 種以字母或數字組成之唯一識別碼，該識別碼必須依國際標準組織(ISO)所訂定之註冊標準加以註冊，並可被用以識別唯一與之對應之憑證政策；憑證政策修訂時，其物件識別碼不必然隨之變更。[憑證實務作業基準應載明事項準則第 2 條第 4 款] (2)向國際標準機構註冊之特別形式的識別

中/英文名詞	定義
	碼，當提及某物件或物件類別時，可以引用此唯一的識別碼做辨識。例如在公開金鑰基礎架構中，可以此識別碼來指明使用的憑證政策及使用的密碼演算法。
線上憑證狀態協定 (Online Certificate Status Protocol, OCSP)	線上憑證狀態協定是 1 種線上憑證檢查協定，使信賴憑證者應用軟體可決定某張憑證之狀態(例如已廢止、有效等)。
線上憑證狀態協定回應伺服器 (OCSP Responder)	由憑證管理中心所授權維運的線上伺服器，並連接至其儲存庫以處理憑證狀態查詢請求。
線上憑證狀態協定裝訂 (OCSP Stapling)	一種 TLS/SSL 憑證狀態請求擴充欄位(TLS Certificate Status Request extension)，可替代線上憑證狀態協定(OCSP)成為另一種檢查 X.509 憑證狀態的方法。 本方法在運作上，網站會事先向 OCSP 回應伺服器取得有「時間限制(例如兩小時)」的 OCSP Response 並暫存；接下來，在每一次的 TLS Handshake 的初始過程中，網站會將此暫存的 OCSP Response 傳送給用戶(通常為瀏覽器)，用戶只需驗證該 OCSP Response 的有效性而不用再向憑證機構發送 OCSP 請求，如此可避免用戶每次連結高流量 TLS 網站都需要向憑證機構詢問其 TLS/SSL 憑證狀態，因此減輕憑證機構的負擔。 此種機制藉由 TLS 網站轉發 OCSP 回應伺服器定期簽發之 TLS/SSL 憑證有效性訊息，也避免 OCSP 回應伺服器可能得知有哪些用戶嘗試瀏覽該 TLS 網站的隱私疑慮。
組織驗證(Organization Validation, OV)	TLS/SSL 憑證核發過程中，除了驗證用戶之網域擁有權或控制權外，並且依照憑證的保證等級識別及鑑別用戶之組織或個人身分。故連結安裝組織驗證型 TLS/SSL 憑證之網站，可提供 TLS 加密通道，知道該網站之擁有者屬於哪一個組織，並確保資料傳遞之完

中/英文名詞	定義
	整性。
特殊安全管道 (Out-of-Band)	不同於現有之線上通訊方式，例如使用實體掛號信與他人進行通訊，此一方式可視為一種特殊安全管道。
私密金鑰 (Private Key)	(1)在簽章金鑰對中，用以產生數位簽章的金鑰。 (2)在加解密金鑰對中，用以對機密資訊解密的金鑰。 在這兩種情境中，此金鑰皆須保密。
公開金鑰 (Public Key)	(1)在簽章金鑰對中，用以驗證數位簽章有效的金鑰。 (2)在加解密金鑰對中，用以對機密資訊加密的金鑰。 在這兩種情境中，此金鑰皆須(一般以數位憑證的形式)公開可得。
公開金鑰基礎建設 (Public Key Infrastructure, PKI)	由法律、政策、規範、人員、設備、設施、技術、流程、稽核和服務所組成之集合，可用於管理憑證及金鑰對。
公開金鑰密碼學標準 (Public Key Cryptography Standards, PKCS)	RSA 資訊安全公司旗下的 RSA 實驗室為促進公開金鑰技術的使用，所發展一系列的公開金鑰密碼編譯標準，廣為業界採用。
合格稽核業者 (Qualified Auditor)	符合 EV SSL Certificate Guidelines 第 17.6 節及 Baseline Requirements 第 8.2 節規定之稽核資格要求，且與受稽方獨立的會計師事務所、法人或個人。
註冊中心(Registration Authority, RA)	通常為憑證機構一部分之個體，負責對憑證的主體做身分識別及鑑別，但不做憑證簽發。
信賴憑證者 (Relying Party)	指信賴所收受之憑證者。[憑證實務作業基準應載明事項準則第 2 條第 6 款]
儲存庫	(1)用以儲存與檢索憑證或其他憑證相關資訊

中/英文名詞	定義
(Repository)	之系統。[憑證實務作業基準應載明事項準則第 2 條第 7 款] (2)包含憑證政策、憑證實務作業基準及憑證相關資訊的資料庫。
徵求修正意見書 (Request for Comments, RFC)	由 IETF 發行的一系列備忘錄，包含網際網路、UNIX 及網際網路社群之標準、協定及程序等，並以編號排定。
保留 IP 位址 (Reserved IP Addresses)	IANA 設定 IPv4 與 IPv6 為保留的位址，參見 http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml 與 http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml。
根憑證機構 (Root Certification Authority, Root CA)	一個公開金鑰基礎建設中最頂層的憑證機構，負責簽發下屬憑證機構憑證及自簽憑證，也稱為憑證總管理中心。
安全插座層(Secure Sockets Layer, SSL)	網景公司(Netscape)推出瀏覽器時所提出的協定，可於傳輸層對網路通信進行加密，並確保傳送資料之完整性以及對於伺服器端與用戶端進行身分鑑別。SSL 協定的優勢在於它與應用層協定(Application Layer Protocol)獨立無關，高階的應用層協定(例如：HTTP、FTP 及 Telnet 等)能直接地建置於 SSL 協定之上。SSL 協定在應用層協定通信之前就已經完成加密演算法、通信密鑰的協商以及伺服器認證工作。此協定之繼任者是傳輸層安全(Transport Layer Security, TLS)協定。
自發憑證 (Self-Issued Certificate)	自發憑證為根憑證機構更換金鑰或憑證政策需要時所簽發之憑證，由兩代(新與舊代)根憑證機構使用其私密金鑰相互簽發，用以建立新舊金鑰間或憑證政策互通時憑證信賴路徑之用。
自簽憑證 (Self-Signed Certificate)	(1)自簽憑證係指憑證的簽發者名稱與憑證的主體名稱相同的一種憑證。亦即使用同一對金鑰對的私密金鑰針對其成配對關係的

中/英文名詞	定義
	公開金鑰與其他資訊所簽發的憑證。 (2)一個公開金鑰基礎建設內的自簽憑證可做為憑證信賴路徑的起源，其簽發對象為根憑證機構本身。 (3)可供信賴憑證者用於驗證根憑證機構簽發之自發憑證、下屬憑證機構憑證、交互憑證以及憑證機構廢止清冊的數位簽章。
簽章憑證 (Signature Certificate)	公開金鑰憑證包含用以驗證數位簽章(而非用於加密資料或其他密碼用途)之公開金鑰。
主體憑證機構 (Subject CA)	對於 1 張憑證機構憑證而言，該憑證的主體中所指的憑證機構即稱為該憑證的主體憑證機構。
下屬憑證機構 (Subordinate CA)	在階層式架構的公開金鑰基礎建設中，憑證由另 1 個憑證機構(上層憑證機構)所簽發，且其活動受限於此另 1 憑證機構的憑證機構。
用戶 (Subscriber)	具下列特性之個體，包括(但不限於)個人、機構、應用程式或網路裝置： (a)憑證中所敘明之主體名稱 (b)擁有與憑證上所載公開金鑰相對應之私密金鑰 (c)本身不簽發憑證給其他方
威脅 (Threat)	對資訊系統可能造成損害(包括損毀、揭露、惡意修改資料或拒絕服務)的任何狀況或事件，可分為內部威脅(Internal Threat) 及外部威脅(External Threat)。內部威脅是指利用授與之權限，透過資料的破壞、揭露、篡改或拒絕服務等方式造成對資訊系統的損害；外部威脅是指來自外部未經授權且對資訊系統具有潛在破壞能力(包括對資料的毀壞、篡改、洩漏，或是造成阻斷服務)的個體。
時戳 (Time-stamp)	由可信賴的權威機構以數位方式簽署，證明某特定數位物件在某特別時間之存在。

中/英文名詞	定義
傳輸層安全(Transport Layer Security, TLS)	由 IETF 將 SSL 3.0 協定制定為 RFC 2246，並將其稱為 TLS 1.0 協定，後續於 RFC 5246 及 RFC 6176 更新版本，亦即 TLS 1.2 協定。2018 年 IETF 公告最新版本 RFC 8446，即 TLS 1.3 協定。
信賴清單 (Trust List)	可信賴憑證之清單，信賴憑證者用以鑑別憑證。
可信賴憑證 (Trusted Certificate)	為信賴憑證者所信賴且經由安全可靠之傳送方式取得的憑證。此類憑證中所包含的公開金鑰用於信賴路徑之起始，又稱為信賴起源。
不斷電系統 (Uninterrupted Power System, UPS)	在電力異常（如停電、干擾或電湧）的情況下不間斷地提供負載設備後備電源，以維持諸如伺服器或交換機等關鍵設備或精密儀器的不間斷運作，防止運算數據遺失，通信網路中斷或儀器失去控制。
驗證 (Validation)	憑證申請者的識別流程。驗證是識別(identification)的子集合，是指建立憑證申請者的身分背景之識別。[RFC 3647]
WebTrust	加拿大會計師公會(Chartered Professional Accountants Canada, CPA Canada)針對憑證機構的 WebTrust Program 項目所制定的規範。加拿大會計師公會也是 WebTrust for CA 系列標章之管理單位。
零值化 (Zeroize)	清除電子式儲存資料之方法，藉由改變資料儲存以防止資料被復原。

1.6.2 縮寫

英文縮寫	英文全稱	中文名詞或定義
AIA	Authority Information Access	憑證機構資訊存取，參見第 1.6.1 節
CA	Certification Authority	憑證機構，參見第 1.6.1 節

CAA	Certification Authority Authorization	授權憑證機構簽發憑證，參見第 1.6.1 節
CARL	Certification Authority Revocation List	憑證機構廢止清冊，參見第 1.6.1 節
CCA	Cross-Certification Agreement	交互認證協議書，參見第 1.6.1 節
CMMI	Capability Maturity Model Integration	能力成熟度模型整合，參見第 1.6.1 節
CP	Certificate Policy	憑證政策，參見第 1.6.1 節
CPS	Certification Practice Statement	憑證實務作業基準，參見第 1.6.1 節
CRL	Certificate Revocation List	憑證廢止清冊，參見第 1.6.1 節
CT	Certificate Transparency	憑證透明化，參見第 1.6.1 節
DN	Distinguished Name	唯一識別名稱
DNS	Domain Name System	網域名稱系統，參見第 1.6.1 節
DV	Domain Validation	網域驗證，參見第 1.6.1 節
EE	End Entities	終端個體
EV	Extended Validation	延伸驗證，參見第 1.6.1 節
FIPS	(U.S. Government) Federal Information Processing Standard	(美國)聯邦資訊處理標準，參見第 1.6.1 節
FQDN	Fully Qualified Domain Name	完全吻合網域名稱，參見第 1.6.1 節
HiPKI RCA	HiPKI Root Certification Authority	HiPKI 憑證總管理中心，參見第 1.6.1 節
IANA	Internet Assigned Numbers Authority	網際網路號碼分配機構，參見第 1.6.1 節
IETF	Internet Engineering Task	網際網路工程任務小組，

	Force	參見第 1.6.1 節
IV	Individual Validation	個人驗證，參見第 1.6.1 節
NIST	(U.S. Government) National Institute of Standards and Technology	(美國)國家標準和技術研究院，參見第 1.6.1 節
OCSP	Online Certificate Status Protocol	線上憑證狀態協定，參見第 1.6.1 節
OID	Object Identifier	物件識別碼，參見第 1.6.1 節
OV	Organization Validation	組織驗證，參見第 1.6.1 節
PIN	Personal Identification Number	個人識別碼
PKCS	Public Key Cryptography Standards	公開金鑰密碼學標準，參見第 1.6.1 節
RA	Registration Authority	註冊中心，參見第 1.6.1 節
RFC	Request for Comments	徵求修正意見書，參見第 1.6.1 節
SSL	Secure Sockets Layer	安全插座層，參見第 1.6.1 節
TLS	Transport Layer Security	傳輸層安全，參見第 1.6.1 節
UPS	Uninterrupted Power System	不斷電系統，參見第 1.6.1 節

2 公布及儲存庫之責任

2.1 儲存庫

儲存庫由 HiPKI RCA 負責管理，公告由 HiPKI RCA 簽發之憑證、憑證機構廢止清冊(Certification Authority Revocation List, CARL)及其他憑證相關資訊，並提供 24 小時全天的服務。HiPKI RCA 儲存庫之網址為：http://eca.hinet.net。如因故無法正常運作，將於 2 個日曆天內恢復正常運作。

2.2 憑證機構之資訊公布

HiPKI RCA 應負責將以下之資訊公布於其儲存庫：

(1) HiPKI 憑證政策及本作業基準

(2) 憑證廢止資訊

(3) HiPKI RCA 之自簽憑證

(4) HiPKI RCA 新舊金鑰互簽之自發憑證

(5) 下屬憑證機構之憑證

(6) 交互認證憑證機構之憑證

(7) 隱私權保護政策

(8) 最近 1 次之外部稽核結果(如第 8.6 節所述)

(9) 相關最新消息

此外，若隸屬於 HiPKI RCA 之下屬憑證機構或與 HiPKI RCA 進行交互認證之交互認證憑證機構之下屬憑證機構提供 TLS/SSL 憑證簽發服務，HiPKI RCA 將要求簽發 TLS/SSL 憑證之憑證機構於其儲存庫公告提供應用軟體供應商測試用的 3 個 TLS/SSL 憑證網址，其分別使用有效、已廢止與已過期的 TLS/SSL 憑證，供應用軟體供應

商各別測試其軟體是否能使用該 TLS/SSL 憑證串連至 HiPKI RCA 的自簽憑證。

2.3 公布之時間或頻率

(1) HiPKI RCA 每年檢視及更新本作業基準，本作業基準新版或修訂後之版本於收到主管機關核准公文後 7 個日曆天內於儲存庫公布本作業基準

(2) HiPKI RCA 所遵循的 HiPKI 憑證政策新版或修訂後之版本於政策管理委員會核定後 7 個日曆天內於儲存庫公布

(3) HiPKI RCA 每天至少簽發兩次憑證機構廢止清冊，公布於儲存庫

(4) 自簽憑證、自發憑證、交互憑證以及下屬憑證機構憑證於簽發及憑證接受後 7 個日曆天內公布於儲存庫

2.4 儲存庫之存取控制

HiPKI RCA 主機與儲存庫主機之間並無任何網路連線，因此 HiPKI RCA 主機簽發的憑證及憑證機構廢止清冊無法直接透過網路傳送到儲存庫主機。在 HiPKI RCA 需要公布簽發的憑證及憑證機構廢止清冊時，由 HiPKI RCA 之相關人員以離線手動方式，將需公布的憑證及憑證機構廢止清冊儲存在可攜式媒體中，再將檔案複製到儲存庫主機中公布。

有關第 2.2 節 HiPKI RCA 公布的資訊，主要提供下屬憑證機構、交互認證憑證機構及信賴憑證者查詢之用，因此開放閱覽與下載，並為保障儲存庫之安全應進行存取控制，且應維持其可接取狀態及可用性。

3 識別及鑑別

3.1 命名

3.1.1 命名種類

HiPKI RCA 簽發憑證之憑證主體名稱為 ITU-T X.500 唯一識別名稱(Distinguished Name, DN)。簽發給 HiPKI RCA 的自簽憑證、自發憑證、簽發給下屬憑證機構之下屬憑證機構憑證及簽發給交互認證憑證機構之交互憑證使用此唯一識別名稱的格式。

3.1.2 命名須有意義

申請成為下屬憑證機構或交互認證憑證機構之憑證主體名稱(Subject)應符合 Baseline Requirements 之規範以及我國法律對該主體命名之相關規定，且足以代表及識別該憑證機構。

3.1.3 用戶之匿名或假名

HiPKI RCA 所簽發給憑證機構的憑證不適用。

3.1.4 不同命名形式之解釋規則

各式命名形式之解釋規則依 ITU-T X.520 名稱屬性定義。

3.1.5 命名之獨特性

HiPKI RCA 將審核申請成為下屬憑證機構與交互認證憑證機構所提出的憑證機構名稱之獨特性，如名稱重複時得要求該憑證機構修改名稱。對於名稱所有權爭議由本公司處理。

HiPKI RCA 的自簽憑證使用以下名稱格式：

C = TW，

O = Chunghwa Telecom Co., Ltd.，

CN = HiPKI Root CA- Gn，其中 n = 1, 2, 3….。

此外，HiPKI RCA 簽發之自簽憑證，其憑證簽發者與憑證主體名稱相同。

3.1.6 商標之辨識、鑑別及角色

下屬憑證機構與交互認證憑證機構提供之憑證主體名稱包含商標或任何受法律保護之姓名、商號、名稱、表徵時，HiPKI RCA 雖不負審查之責，但其命名必須符合我國商標法、公平交易法及其相關規定，HiPKI RCA 不保證憑證主體名稱商標之認可、驗證、合法及唯一性，相關之糾紛或仲裁處理，非 HiPKI RCA 之權責範圍，由下屬憑證機構與交互認證憑證機構向相關主管機關或法院提出申請。

3.2 初始身分驗證

3.2.1 證明擁有私密金鑰之方式

憑證機構申請憑證時，HiPKI RCA 檢驗憑證機構之私密金鑰與將記載於憑證中之公開金鑰是否成對。由該憑證機構產生 1 個 PKCS#10 憑證申請檔，HiPKI RCA 使用該憑證機構的公開金鑰檢驗簽章，以證明該憑證機構擁有相對應之私密金鑰。

3.2.2 組織身分鑑別

HiPKI RCA 之身分鑑別，由本公司召開政策管理委員會會議審核。

由本公司自行設立之憑證機構成為下屬憑證機構時(例如：HiPKI

EV TLS CA)，其身分鑑別由本公司召開政策管理委員會會議審核。

非本公司自行設立之憑證機構，由憑證機構提交交互認證申請書，申請書中包含組織名稱、所在地及代表人等足以識別該組織之資料。HiPKI RCA 將確認該組織是否存在，驗證申請書之真偽、代表人身分及代表人是否有權代表該組織，代表人應親臨本公司辦理憑證申請。

如下屬憑證機構核發之憑證用途為電子郵件之簽章及加密，下屬憑證機構應鑑別該組織身分並驗證該組織確實擁有或被授權使用記載於憑證內之電子郵件信箱。

如下屬憑證機構核發之憑證用途為 TLS 伺服器加密傳輸，下屬憑證機構應遵循 Baseline Requirements，下屬憑證機構應鑑別憑證申請者具有其網域名稱(domain name)擁有權或控制權，若該 TLS/SSL 憑證屬於組織驗證型，下屬憑證機構應鑑別該組織之身分並驗證該組織確實擁有或被授權使用記載於憑證中之完全吻合網域名稱(Fully Qualified domain name)，下屬憑證機構得與可信賴之資料庫登記資料進行比對。若該 TLS/SSL 憑證屬於個人驗證型，下屬憑證機構應鑑別該自然人之身分並驗證該自然人確實擁有或被授權使用記載於憑證內之完全吻合網域名稱，下屬憑證機構得與可信賴之資料庫登記資料進行比對。若該 TLS/SSL 憑證屬於延伸驗證型，下屬憑證機構應依照 EV SSL Certificate Guidelines 鑑別該組織之身分並驗證該組織確實擁有或被授權使用記載於憑證內之完全吻合網域名稱，下屬憑證機構得與可信賴之資料庫登記資料進行比對。

如下屬憑證機構核發之憑證用途為時戳伺服器之簽章與加密，下屬憑證機構應鑑別該組織之身分並驗證該組織記載於憑證內之時戳伺服器的應用軟體名稱是否恰當。

如下屬憑證機構核發之憑證用途為程式碼簽章(code signing)，下屬憑證機構應鑑別該組織之身分並驗證該組織確實與記載於憑證內之組織名稱相符。

3.2.3 個人身分鑑別

本公司所設立之憑證機構不適用。非本公司所設立之憑證機構，必須以正式書面文件指派代表人(被授權辦理交互認證申請的個人)申請憑證機構之憑證，鑑別程序如下：

(1)核對書面證件：

在申請憑證時，代表人應出示中華民國國民身分證正本或護照，供HiPKI RCA鑑別代表人之身分。代表人的身分證字號、姓名及戶籍地址等資料，需與憑證機構提交的申請資料進行比對。

(2)提交代表人之授權證明書。

代表人必須親自證明其身分。

3.2.4 未經驗證之用戶資訊

簽發保證等級第 4、3 與 2 級或 TLS/SSL 憑證的憑證機構不適用。

憑證機構可不需要驗證保證等級第 1 級的個人憑證其通用名稱(Common Name)是否為憑證申請者的法定名稱。

3.2.5 授權之確認

當某個個人(憑證申請代表人)與憑證主體之名稱有關連，進行憑證生命週期活動如憑證申請或廢止請求時，HiPKI RCA 應進行授權的

確認(Validation of Authority)，確認該個人可代表憑證主體，例如：

(1) 藉由第三方之身分鑑別服務或資料庫驗證、政府機關或有權責及公信力之團體的文書、公證人、律師或會計師的認證文書(Attestation Letter)或憑證機構到點訪視證明組織之存在。

(2) 藉由電話、郵件、電子郵件等聯絡方式(從其他非憑證申請代表人的來源取得)或其他相當之程序確認該個人確實任職於該憑證主體(某組織或公司)得到授權代表該憑證主體。

(3) 藉由臨櫃面對面核對身分或其他可信賴的通訊方式確認該個人代表組織。

3.2.6 互運之準則

目前 HiPKI RCA 未和任何其他公開金鑰基礎建設的根憑證機構簽署交互認證憑證。

3.2.7 資料來源正確性

在使用任何資料來源作為可靠資料來源之前，HiPKI RCA應評估此來源的可靠性、正確性和對變更或偽造的抵抗性。HiPKI RCA在評估過程中應考慮下列事項：

(1) 所提供資訊的存在時間。

(2) 資訊來源的更新頻率。

(3) 資料提供者和資料收集的目的。

(4) 資料可用性的公用可存取性。

(5) 偽造或變更資料的相對困難性。

由 HiPKI RCA、其擁有者或其附屬公司所維護的資料庫，如果資料庫的主要目的是為了滿足 Baseline Requirements 第 3.2 節的驗證要求而蒐集的資訊，則不符合可靠資料來源。

3.3 金鑰更換請求之識別及鑑別

憑證之金鑰更換係指簽發 1 張與舊憑證具有相同特徵及保證等級的新憑證，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，亦可能被指定不同的有效期限。

下屬憑證機構或交互認證憑證機構更換金鑰時,應向 HiPKI RCA 重新申請憑證，HiPKI RCA 依照第 3.2.2 節規定，對於重新申請憑證之憑證機構進行識別及鑑別。

3.3.1 例行性金鑰更換之識別及鑑別

HiPKI RCA 的自簽憑證、自發憑證及下屬憑證機構的憑證到期後不准展期，依照第 3.2 節規定，重新辦理初始身分驗證。

3.3.2 憑證廢止後金鑰更換之識別及鑑別

憑證機構之憑證廢止後，新憑證申請之識別與鑑別程序依照第 3.2 節規定，重新辦理初始身分驗證。

3.4 憑證廢止請求之識別及鑑別

HiPKI RCA 自簽憑證、下屬憑證機構憑證與交互認證憑證廢止申請之鑑別程序與第 3.2 節規定相同。

4 憑證生命週期營運規定

4.1 憑證申請

4.1.1 憑證之申請者

憑證申請者包括 HiPKI RCA、下屬憑證機構或是本基礎建設外之根憑證機構。

4.1.2 註冊程序及責任

4.1.2.1 HiPKI RCA 之義務

(1) 依據憑證政策保證等級第 4 級規定與本作業基準運作

(2) 訂定下屬憑證機構申請與憑證機構的交互認證申請程序

(3) 執行下屬憑證機構申請與憑證機構交互認證申請之識別與鑑別程序

(4) 簽發及公布憑證

(5) 廢止憑證

(6) 簽發及公布憑證機構廢止清冊

(7) 簽發及提供線上憑證狀態協定(Online Certificate Status Protocol, OCSP)回應訊息

(8) 執行憑證機構人員之識別與鑑別程序

(9) 安全產製 HiPKI RCA 之私密金鑰

(10)保護 HiPKI RCA 之私密金鑰

(11)執行 HiPKI RCA 自簽憑證之金鑰更換及其自發憑證之簽發

(12)受理下屬憑證機構之憑證註冊及廢止申請

(13)受理交互認證憑證機構之交互憑證註冊及廢止申請

4.1.2.2 下屬憑證機構之義務

(1) 遵守本作業基準之規定，如未遵守導致信賴憑證者遭受損害時，應負損害賠償責任

(2) HiPKI RCA 簽發之憑證，依據憑證政策的規定，不同保證等級有不同之適用範圍，下屬憑證機構於提出憑證申請時，必須敘明所申請憑證之保證等級

(3) 下屬憑證機構申請憑證應依照第 4.2 節之程序進行申請，並確認申請資料之正確性

(4) 在核可下屬憑證機構之申請及 HiPKI RCA 簽發憑證後，下屬憑證機構應依照第 4.4 節規定接受憑證

(5) 下屬憑證機構在接受 HiPKI RCA 所簽發之憑證後，即表示已確認憑證內容資訊之正確性，並依照第 4.5 節規定使用憑證

(6) 下屬憑證機構應依照第 6 章規定，自行產製私密金鑰

(7) 下屬憑證機構應妥善保管及使用私密金鑰

(8) 使用與憑證之公開金鑰相對應之私密金鑰簽署之數位簽章即為下屬憑證機構之數位簽章，下屬憑證機構在產生數位簽章時，必須確認已接受該下屬憑證機構憑證，且該憑證仍在有效期間並未被廢止

(9) 下屬憑證機構如發生第 4.9.1 節廢止憑證之事由(如私密金鑰資料外洩或遺失)，必須廢止憑證時，應立即通知 HiPKI RCA，並依照第 4.9 節規定辦理憑證暫時停用或廢止，但下屬憑證機構仍應承擔憑證廢止狀態未被公布前所有使用該憑證之法律責任

(10) HiPKI RCA 如因故無法正常運作時，下屬憑證機構應儘速尋求其他途徑完成與他人應為之法律行為，不得以 HiPKI RCA

無法正常運作，作為抗辯他人之事由

4.1.2.3 交互認證憑證機構之義務

(1) 遵守本作業基準及交互認證協議之規定，如未遵守導致信賴憑證者遭受損害時，應負損害賠償責任

(2) HiPKI RCA 簽發之憑證，依據憑證政策的規定，不同保證等級有不同之適用範圍，憑證機構於提出交互認證申請時，必須敘明所申請憑證之保證等級

(3) 憑證機構申請憑證應依照第 4.2 節之程序進行交互認證申請，並確認申請資料之正確性

(4) 在核可憑證機構之交互認證申請及 HiPKI RCA 簽發憑證後，憑證機構應依照第 4.4 節規定接受憑證

(5) 憑證機構在接受 HiPKI RCA 所簽發之憑證後，即表示已確認憑證內容資訊之正確性，並依照第 4.5 節規定使用憑證

(6) 申請交互認證之憑證機構應依照第 6 章規定，自行產製私密金鑰

(7) 交互認證憑證機構應妥善保管及使用私密金鑰

(8) 使用與憑證之公開金鑰相對應之私密金鑰簽署之數位簽章即為憑證機構之數位簽章，憑證機構在產生數位簽章時，必須確認已接受該憑證，且該憑證仍在有效期間並未被廢止

(9) 憑證機構如發生第 4.9.1 節廢止憑證之事由(如私密金鑰資料外洩或遺失)，必須廢止憑證時，應立即通知 HiPKI RCA，並依照第 4.9 節規定辦理憑證暫時停用或廢止，但憑證機構仍應承擔憑證廢止狀態未被公布前所有使用該憑證之法律責任

(10) HiPKI RCA 如因故無法正常運作時，憑證機構應儘速尋求其

他途徑完成與他人應為之法律行為，不得以 HiPKI RCA 無法正常運作，作為抗辯他人之事由

4.2 憑證申請之程序

本基礎建設中所有層級之下屬憑證機構，除非經其上層憑證機構之同意，否則不得接受其他憑證機構申請成為其下層憑證機構。

HiPKI RCA 簽發交互憑證給本基礎建設外之根憑證機構前，應由政策管理委員會與該憑證機構協商以決定是否承認該根憑證機構簽發給其他憑證機構的交互憑證。

4.2.1 執行識別及鑑別

4.2.1.1 初始

(1) 初始申請

本公司所設立之憑證機構，由本公司召開政策管理委員會會議審核 PKCS#10 憑證申請檔及欲簽發之憑證效期與憑證主體名稱等資訊，非本公司設立之憑證機構須送交互認證申請書、憑證實務作業基準及 PKCS#10 憑證申請檔等資料，如憑證機構遵循的憑證政策非 HiPKI 憑證政策時，應另檢附所遵循的憑證政策。外部下屬憑證機構或非本基礎建設之根憑證機構應檢附最新之時間點查核報告(Point-in-time Audit Report)或/及區間查核報告(Period of time Audit Report)。簽發 TLS/SSL 憑證之憑證機構另應檢附 Baseline Requirement Assessment 表。

(2) 身分識別及鑑別

依照第 3.2.2 節規定，執行申請 HiPKI RCA、下屬憑證機構

或交互認證之憑證機構的身分識別及鑑別程序。

(3) 執行以下檢查程序

確認申請成為下屬憑證機構或交互認證之憑證機構與 HiPKI RCA 間沒有技術上不相容之問題。

如申請交互認證之憑證機構遵循的憑證政策非 HiPKI 憑證政策時，應檢查其憑證政策與 HiPKI RCA 在憑證政策的對應關係。

檢查憑證機構之憑證實務作業基準是否遵循各該機構所引用的憑證政策。

檢驗初始申請交付的 PKCS#10 憑證申請檔，以確認是否可以完成實際的交互認證作業。

4.2.2 憑證申請之批准或拒絕

4.2.2.1 審查申請(Examination)

HiPKI RCA 提出自簽憑證申請時，將召開政策管理委員會會議審查。

憑證機構提出下屬憑證機構憑證申請時，將召開政策管理委員會會議審查。

憑證機構提出交互認證申請時，將召開政策管理委員會會議，審查申請之憑證機構提交之相關文件資料及 HiPKI RCA 之檢查結果，以決定憑證機構與 HiPKI RCA 交互認證之妥適性。最後依該委員會之決議，決定進入下一階段，或要求補送資料，或駁回申請。

4.2.2.2 協議(Arrangement)

本公司設立之憑證機構，不用簽署交互認證協議書。

非本公司設立之憑證機構提出交互認證申請時，將召開會議通知申請交互認證之憑證機構參加，並進行以下步驟：

(1) 身分識別與鑑別

會議開始前，依照第 3.2.3 節規定，執行申請交互認證之憑證機構代表人的身分識別與鑑別程序

(2) 與申請交互認證之憑證機構協商必須遵守之條款與條件

(3) 核定是否與申請交互認證之憑證機構進行交互認證，如同意則與申請交互認證之憑證機構簽署交互認證協議書(Cross-Certification Agreement, CCA)

(4) 進入簽發憑證程序

4.2.3 處理憑證申請之時間

憑證機構提出憑證申請所提交的資料齊全且符合憑證政策及 HiPKI RCA 實務作業基準，技術與 HiPKI RCA 相容下，經政策管理委員會會議審查通過後，HiPKI RCA 應於 7 個日曆天內完成憑證之簽發。

4.3 憑證簽發

4.3.1 憑證簽發時憑證機構之作業

HiPKI RCA 依照政策管理委員會會議決議(會議紀錄)簽發自簽憑證與自發憑證。

HiPKI RCA 將簽發 1 張自簽憑證(Self-Signed Certificate)，此憑證依照第 6.1.4 節規定傳送給信賴憑證者。

HiPKI RCA 依照政策管理委員會會議核定結果(會議紀錄)決定是否簽發下屬憑證機構憑證或交互認證憑證機構之交互憑證。

4.3.2 憑證機構對憑證申請者之憑證簽發通知

如核可憑證申請將通知下屬憑證機構或交互認證之憑證機構，由HiPKI RCA 執行憑證簽發之相關工作。憑證簽發後，如為非本公司設立之憑證機構，本公司將發函通知該憑證機構並檢附簽發的憑證。

如未核可憑證申請，將發函通知申請成為下屬憑證機構或交互認證之憑證機構，並說明未核可的理由。

4.4 憑證接受

4.4.1 構成接受憑證之事由

HiPKI RCA 確認自簽憑證與自發憑證之資訊無誤後，經內部簽核程序將自簽憑證與自發憑證公布於儲存庫。

申請成為下屬憑證機構或交互認證之憑證機構在收到核可憑證通知後，必須檢查所附的憑證，確認該憑證內容之正確性，如憑證內容無誤，應通知 HiPKI RCA，非本公司設立之憑證機構必須簽署憑證接受確認文件，並函復本公司，以完成憑證接受程序。

如憑證機構於 30 個日曆天內未能函復憑證接受確認文件，則視為拒絕接受憑證，HiPKI RCA 將廢止該憑證，並不另行公布。

4.4.2 憑證機構對簽發憑證之發布

HiPKI RCA 在收到憑證接受確認文件後，將簽發給下屬憑證機構之憑證機構憑證或簽發給交互認證憑證機構之交互憑證公布於儲存庫。

本公司設立之下屬憑證機構經內部簽核程序將下屬憑證機構憑證公布於儲存庫。

4.4.3 憑證機構對其他個體之憑證簽發通知

HiPKI RCA 若有新簽發的自簽憑證、自發憑證、下屬憑證機構憑證或交互憑證，將會依照各作業系統、瀏覽器與軟體平台之根憑證計畫(Root Certificate Program)之規定進行通知，例如上載相關憑證至 Common CA Database (CCADB)。

4.5 金鑰對及憑證之用途

4.5.1 用戶私密金鑰及憑證之用途

用戶係指已申請並取得憑證之個體，對組織與個人而言係指憑證主體所記載的名稱，並擁有與憑證之公開金鑰相對應之私密金鑰的個體。對於財產類別(例如應用程式及硬體設備)而言，由於財產本身無行為能力，因此憑證用戶為申請憑證的個人或組織。用戶金鑰對的產製應符合憑證政策第 6.1.1 節之規定，並且用戶必須獨自擁有控制憑證相對應私密金鑰的權力與能力，用戶本身不簽發憑證給其他方。用戶應保護其私密金鑰不被他人未經授權的使用或揭露，且只使用其私密金鑰於正確的金鑰用途(於憑證之擴充欄位有註記金鑰用途)。用戶必須依據憑證所記載的憑證政策正確地應用憑證。

4.5.2 信賴憑證者公開金鑰及憑證之用途

信賴憑證者係指相信憑證主體名稱與公開金鑰間連結關係之第三人。信賴憑證者應使用符合 ITU-T X.509、RFC、Baseline Requirements 或 EV SSL Certificate Guidelines 相關標準或規範的軟體。

信賴憑證者必須依照相對的憑證機構憑證及憑證狀態資訊，以驗證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：

(1) 驗證具有數位簽章的電子文件之完整性。

(2) 驗證文件簽章產生者的身分。

(3) 與用戶間建立安全之通訊管道。

前述憑證狀態資訊可透過憑證機構廢止清冊、憑證廢止清冊或線上憑證狀態協定查詢服務取得。憑證機構廢止清冊或憑證廢止清冊下載網址可於憑證的憑證廢止清冊發布點(CRL Distribution Point, CDP)擴充欄位中取得；線上憑證狀態協定查詢服務網址可於憑證的憑證機構資訊存取(Authority Information Access, AIA)擴充欄位中取得。此外，信賴憑證者也應檢驗簽發憑證機構與用戶憑證之憑證政策，確認憑證之保證等級。

4.6 憑證展期

憑證機構的憑證不可展期，只有用戶的憑證才可展期。

4.6.1 憑證展期之情況

不適用。

4.6.2 憑證展期之申請者

不適用。

4.6.3 憑證展期之程序

不適用。

4.6.4 對用戶憑證展期之簽發通知

不適用。

4.6.5 構成接受展期之憑證的事由

不適用。

4.6.6 憑證機構對展期之憑證的發布

不適用。

4.6.7 憑證機構對其他個體之憑證簽發通知

不適用。

4.7 憑證機構憑證之金鑰更換

4.7.1 憑證金鑰更換之情況

下屬憑證機構在以下 3 種情形會更換金鑰並由 HiPKI RCA 簽發新的下屬憑證機構憑證：

(1) 目前使用之金鑰生命週期結束。

(2) 目前使用之金鑰的安全性有問題時(例如懷疑或確定金鑰被破解)。

(3) 憑證所使用之密碼演算法安全性有疑慮或因國際間採預防性措施提前淘汰(例如憑證機構與瀏覽器論壇於 103 年 10 月決議淘汰 SHA-1 雜湊函數演算法)。

交互認證憑證機構在以下兩種情形會更換金鑰並由 HiPKI RCA 簽發新的交互認證憑證：

(1) 目前使用之金鑰生命週期結束。

(2) 目前使用之金鑰的安全性有問題時(例如懷疑或確定金鑰被破解)。

下屬憑證機構應依照第 6.3.2.2 節規定定期更換其金鑰對。下屬

憑證機構更換金鑰對後，依照第 4.1 及第 4.2 節規定向 HiPKI RCA 申請新的憑證。

交互認證憑證機構應依照第 6.3.2.2 節規定定期更換其金鑰對。交互認證憑證機構更換金鑰對後，依照第 4.1 及第 4.2 節規定向 HiPKI RCA 申請新的憑證。

簽發保證等級第 2、第 3 及第 4 級之憑證的憑證機構，如其憑證沒有被廢止，HiPKI RCA 可於該憑證機構簽發用戶憑證之私密金鑰使用期限到期前 2 個月開始受理其更換金鑰並申請新的憑證，申請新憑證之程序依照第 4.2 節規定辦理。

憑證機構的憑證如因國際間預防性之安全控制措施或是其他經政策管理委員會決議通過之事由而在該憑證機構簽發用戶憑證之私密金鑰使用期限尚未到期前，得依照第 4.2 節規定提出新憑證之申請。

4.7.2 更換憑證金鑰之申請者

憑證申請者包括下屬憑證機構或是本基礎建設外之根憑證機構。

4.7.3 憑證金鑰更換之程序

憑證機構更換金鑰時，應向 HiPKI RCA 重新申請憑證，HiPKI RCA 處理金鑰更換時之程序必須依照第 3.1、3.2、3.3、4.1 及 4.2 節之規定辦理。

4.7.4 對憑證機構憑證金鑰更換之簽發通知

依照第 4.3.2 節規定辦理。

4.7.5 構成接受金鑰更換之憑證的事由

依照第 4.4.1 節規定辦理。

4.7.6 憑證機構對金鑰更換之憑證的發布

依照第 4.4.2 節規定辦理。

4.7.7 憑證機構對其他個體之憑證簽發通知

依照第 4.4.3 節規定辦理。

4.8 憑證變更

4.8.1 憑證變更之情況

憑證變更係指對同一憑證主體提供 1 張新的憑證，其記載資訊和舊的憑證有些許不同(例如新增憑證政策物件識別碼於下屬憑證機構憑證或自發憑證之憑證政策擴充欄位)，新的憑證有新的憑證序號，但新憑證和舊憑證的公開金鑰及到期日相同。

4.8.2 憑證變更之申請者

憑證申請者包括 HiPKI RCA、下屬憑證機構或是本基礎建設外之根憑證機構。

4.8.3 憑證變更之程序

依照第 4.2 節規定辦理。

4.8.4 對憑證機構憑證變更之簽發通知

依照第 4.3.2 節規定辦理。

4.8.5 構成接受變更之憑證的事由

依照第 4.4.1 節規定辦理。

4.8.6 憑證機構對變更之憑證的發布

依照第 4.4.2 節規定辦理。

4.8.7 憑證機構對其他個體之憑證簽發通知

不做規定。

4.9 憑證廢止及停用

HiPKI RCA 不提供停用與恢復使用服務，憑證廢止資訊公布於 HiPKI RCA 儲存庫。

對於已過期之憑證，HiPKI RCA 得不受理該憑證之廢止申請，但對於過期前被廢止之憑證，HiPKI RCA 應將其廢止資訊列入憑證機構廢止清冊中，待憑證效期到期後始可移除。

4.9.1 憑證廢止之情況

HiPKI RCA 在以下情況(包含但不限)必須提出憑證廢止申請：

(1) 懷疑或證實私密金鑰遭到破解，包括私密金鑰資料外洩或遺失。

(2) 憑證不再需要使用，包括 HiPKI RCA 終止服務。

以下幾種情況發生時，HiPKI RCA 應於 7 天內廢止下屬憑證機構或交互認證憑證機構之憑證：

(1) 下屬憑證機構或交互認證憑證機構以書面提交憑證廢止申請

(2) 下屬憑證機構或交互認證憑證機構告知憑證機構原有之憑證請求未經授權

(3) 憑證機構證實下屬憑證機構或交互認證憑證機構之私密金鑰遭破解或違反第 6.1.5 及第 6.1.6 節對於金鑰之長度及品質檢

測之規定，且該私密金鑰與下屬憑證機構或交互認證憑證機構憑證中所記載之公開金鑰成配對關係

(4) 證實下屬憑證機構或交互認證憑證機構之憑證遭到誤用

(5) 憑證未依憑證政策或憑證實務作業基準之規定程序簽發時

(6) 憑證中所記載之資訊不正確(inaccurate)或已變更

(7) 下屬憑證機構或交互認證憑證機構終止營運，且未安排其他憑證機構承接以提供憑證廢止服務

(8) 下屬憑證機構或交互認證憑證機構之簽發憑證的權力已逾期、被廢止或被中止，且不再維運儲存庫、公布憑證廢止清冊或提供線上憑證狀態協定查詢服務

(9) 憑證政策或本作業基準所規定應廢止項目

如憑證之憑證主體資訊必須變更時，由 HiPKI RCA 審查是否同意廢止憑證申請。HiPKI RCA 依照上述應廢止憑證之情況，得逕行廢止下屬憑證機構或交互認證憑證機構之憑證。

4.9.2 憑證廢止之申請者

下屬憑證機構或交互認證憑證機構得於憑證有效期限內向 HiPKI RCA 提出憑證廢止請求。

此外，應用軟體供應商、信賴憑證者以及其他第三方的組織可以提供憑證問題報告，向 HiPKI RCA 告知合理之原因以廢止憑證。HiPKI RCA 接收到憑證問題報告後，依第 4.9.5 節之規定，確認憑證廢止請求是否成立。

4.9.3 憑證廢止之程序

4.9.3.1 初始

(1) 初始申請

發函提出申請，並檢具憑證廢止申請書。

(2) 身分識別與鑑別

依照第3.2.2節規定，執行HiPKI RCA、下屬憑證機構或交互認證憑證機構的身分識別與鑑別程序。

(3) 審查申請

審查提交之相關文件資料，以決定憑證廢止申請之妥適性。

(4) 決定點

決定進入下一階段，或要求補送資料，或發函通知下屬憑證機構或該交互認證憑證機構未核可憑證廢止申請，並明確說明未核可之理由。

4.9.3.2 廢止憑證

HiPKI RCA 最遲於下次公布憑證機構廢止清冊前，將廢止憑證加入憑證機構廢止清冊中，並公告於儲存庫。憑證廢止後將發函通知下屬憑證機構或交互認證憑證機構，儲存庫公告的憑證狀態資訊將包括廢止的憑證，直到憑證到期為止。

4.9.3.3 憑證問題回應機制

HiPKI RCA 提供憑證問題回報與指引說明。憑證機構、應用軟體供應商、信賴憑證者以及其他第三方組織可至 HiPKI RCA 網站，取得有關回報憑證問題的指引說明，並可依該說明向 HiPKI RCA 進行憑證問題的回報。

4.9.4 憑證廢止請求之寬限期

HiPKI RCA、下屬憑證機構或交互認證憑證機構如發生第 4.9.1 節之情形，最遲應於 10 個日曆天內提出憑證廢止申請，並且儘可能於 HiPKI RCA 下一次簽發憑證機構廢止清冊前提出。

如發生第 4.9.1 節中，毋須事先經過下屬憑證機構或交互認證憑證機構同意，HiPKI RCA 得逕行廢止憑證之情形，則 HiPKI RCA 可於憑證廢止事由確認成立後，逕行提出憑證廢止申請，並通知下屬憑證機構或交互認證憑證機構。

4.9.5 憑證機構處理憑證廢止請求之處理期限

HiPKI RCA 在接收到憑證問題報告的 24 小時內，應調查有關的事實及情況，並提供 1 份初步的調查報告給憑證機構及報告回報者。

在審視有關的事實及情況後，HiPKI RCA 應與憑證機構及憑證問題報告(或其他憑證廢止通知)之回報者共同確認該憑證廢止請求是否成立。若憑證廢止請求經確認後成立，應於第 4.9.1 節規範之處理期限內完成憑證廢止作業。憑證廢止之處理期限應考量下述準則：

(1) 聲稱問題的內容(包括範圍、過程、嚴重程度、重要性及危害的風險等)

(2) 憑證廢止的後果(對憑證機構或信賴憑證者直接或間接的影響)

(3) 該憑證機構憑證的憑證問題報告數量

(4) 提出憑證問題報告的單位

(5) 相關的法律條文

4.9.6 信賴憑證者檢查憑證廢止之規定

信賴憑證者在使用 HiPKI RCA 所簽發之下屬憑證機構憑證、交

互憑證或自發憑證前，應先檢驗 HiPKI RCA 公布之憑證機構廢止清冊或線上憑證狀態協定回應訊息，以確定該憑證是否有效。

信賴憑證者應檢驗憑證之廢止時間、憑證機構廢止清冊或線上憑證狀態協定回應訊息(Online Certificate Status Protocol Response, OCSP Response)之簽章的真偽、完整性及有效性。例如，使用憑證機構廢止清冊時，信賴憑證者應檢查憑證機構廢止清冊的簽發者唯一識別名稱是否與 HiPKI RCA 自簽憑證的主體唯一識別名稱相符，並以 HiPKI RCA 自簽憑證所記載的公開金鑰檢驗憑證機構廢止清冊的簽章。

信賴憑證者應檢查憑證機構廢止清冊是否為最新公布的資訊，憑證機構廢止清冊的生效時間(thisUpdate)欄位記載 HiPKI RCA 更新該憑證機構廢止清冊資訊的時間，下次更新時間(nextUpdate)欄位記載下次 HiPKI RCA 預計更新憑證機構廢止清冊資訊的時間。信賴憑證者檢驗憑證機構廢止清冊時，若系統時間(此系統須定期校時)已經超過憑證機構廢止清冊的下次更新時間，則表示該憑證機構廢止清冊已非最新資訊，信賴憑證者應至儲存庫下載最新的憑證機構廢止清冊。

倘若信賴憑證者欲檢驗舊有資料(例如已經歸檔的資料)，則應檢查當初資料產生時的憑證機構廢止清冊是否為當期的憑證機構廢止清冊。

4.9.7 憑證廢止清冊之簽發頻率

憑證機構廢止清冊之簽發頻率為每天至少 2 次，有效期限不超過 36 小時，更新後之憑證機構廢止清冊公布於儲存庫。由於憑證機構廢止清冊尚未過期前，HiPKI RCA 即可能簽發新的憑證機構廢止清冊，因此新憑證機構廢止清冊的效期與舊的憑證機構廢止清冊的效期

會可能有所重疊，在效期重疊期間，即使舊的憑證機構廢止清冊尚未過期，信賴憑證者仍可至 HiPKI RCA 儲存庫取得新的憑證機構廢止清冊。

當有憑證被廢止時，HiPKI RCA 會於完成憑證廢止作業後的 24 小時內重新簽發憑證機構廢止清冊，將廢止之憑證資訊加入憑證機構廢止清冊中，並公告於儲存庫。

4.9.8 憑證廢止清冊發布之最大延遲時間

HiPKI RCA 最遲在憑證廢止清冊所記載之下次更新時間(nextUpdate)前將憑證機構廢止清冊公布。

4.9.9 線上憑證廢止及狀態查驗之可用性

HiPKI RCA 以憑證機構廢止清冊及線上憑證狀態協定查詢服務等方式提供憑證之狀態查詢。

HiPKI RCA 由線上憑證狀態協定回應伺服器(Online Certificate Status Protocol Responder, OCSP Responder)提供符合 RFC 6960 及 RFC 5019 標準規範的線上憑證狀態協定回應訊息，HiPKI RCA 使用簽章用私密金鑰簽發安全強度至少為 RSA 2048 w/SHA-256 之線上憑證狀態協定回應伺服器之憑證，以供信賴憑證者驗證線上憑證狀態協定回應訊息的數位簽章，確認資料來源之完整性與可信度。其中，線上憑證狀態協定回應伺服器之伺服器憑證須包含符合 RFC 6960 規範之擴充欄位「id-pkix-ocsp-nocheck」。

4.9.10 線上憑證廢止查驗之規定

如信賴憑證者無法依照第 4.9.6 節之規定查詢憑證機構廢止清冊，則應使用第 4.9.9 節之線上憑證狀態協定查詢服務，檢驗所使用的憑證是否有效。

HiPKI RCA 提供線上憑證狀態協定查詢服務，其可支援符合 RFC 6960 及 RFC 5019 標準規範所述之 HTTP-based 的 POST 與 GET 方法，且該服務至少每 12 個月會更新與確認自發憑證、下屬憑證機構憑證及交互憑證的狀態資訊；若自發憑證、下屬憑證機構憑證或交互憑證被廢止，則於憑證廢止後 24 小時內須更新憑證狀態資訊，以供線上憑證狀態協定查詢服務提供最新且正確的憑證狀態資訊。

線上憑證狀態協定查詢封包內含之憑證序號可分為三種，分別為「已分配(Assigned)」、「已保留(Reserved)」及「未使用(Unused)」。「已分配」之憑證序號意即為 HiPKI RCA 已簽發憑證之憑證序號，「已保留」之憑證序號為簽發 TLS/SSL 憑證所需之預簽憑證(Precertificate)的憑證序號，不符合前述條件之憑證序號皆屬於「未使用」之憑證序號。其中，由於 HiPKI RCA 不提供用戶憑證之簽發，故亦未簽發預簽憑證。換言之，HiPKI RCA 之線上憑證狀態協定回應伺服器可處理之線上憑證狀態協定查詢封包應僅包含「已分配」或「未使用」等兩種憑證序號。

若線上憑證狀態協定回應伺服器接收到查詢「已分配」之憑證序號的線上憑證狀態協定查詢封包時，應依該憑證序號所對應之憑證當時之狀態回覆；若線上憑證狀態協定回應伺服器接收到查詢「未使用」之憑證序號的線上憑證狀態協定查詢封包時，不可回覆其狀態為「正常(Good)」，並且 HiPKI RCA 應監督線上憑證狀態協定回應伺服器對於這類請求的回覆是否符合其安全回應程序。

4.9.11 廢止公告之其他發布形式

為了加速高流量網站的 TLS/SSL 憑證之驗證，以完成即時線上 TLS/SSL 憑證狀態之驗證作業，HiPKI RCA 支援線上憑證狀態協定裝訂(OCSP Stapling)運作。

4.9.12 金鑰被破解時之特殊規定

如下屬憑證機構或交互認證憑證機構之私密金鑰被破解時，HiPKI RCA 將於公布之憑證機構廢止清冊中註明該憑證廢止的原因為金鑰被破解。

4.9.13 憑證停用之情況

不提供停用憑證服務。

4.9.14 憑證停用之申請者

不適用。

4.9.15 憑證停用之程序

不適用。

4.9.16 憑證停用期間之限制

不適用。

4.10 憑證狀態服務

4.10.1 操作特性

HiPKI RCA 提供憑證機構廢止清冊，並於自發憑證、下屬憑證機構憑證以及交互憑證中註記憑證機構廢止清冊發布點。此外，HiPKI RCA 亦提供線上憑證狀態協定查詢服務。

在憑證機構廢止清冊或線上憑證狀態協定回應訊息中的憑證廢止資訊，須至該廢止憑證的憑證效期已到期後始可移除。

4.10.2 服務可用性

HiPKI RCA 維運 7 天 x 24 小時不中斷之儲存庫系統，以提供憑

證機構廢止清冊與線上憑證狀態協定查詢服務的功能。在正常工作條件下，前述兩種憑證狀態查詢服務功能的回覆時間須在 10 秒內。

HiPKI RCA 具備 7 天 x 24 小時的回應機制，以因應高優先權的憑證問題報告(High-Priority Certificate Problem Report)，HiPKI RCA 可視案件情況向執法當局舉發，並得廢止發生問題的憑證。

4.10.3 可選功能

不做規定。

4.11 訂購終止

訂購終止(End of Subscription)是指下屬憑證機構或交互認證機構終止使用 HiPKI RCA 的服務。

HiPKI RCA 應允許下屬憑證機構或交互認證機構藉由廢止憑證或憑證到期而不做更新或是交互認證協議書約定條款失效而終止其對於憑證服務之訂購。

4.12 私密金鑰託管及回復

4.12.1 金鑰託管及回復之政策及實務

HiPKI RCA 簽章用之私密金鑰不可被託管(Escrowed)。HiPKI RCA 亦並未支援下屬憑證機構、交互認證機構以及用戶私密金鑰託管與回復。

4.12.2 會議金鑰封裝及回復之政策及實務

HiPKI RCA 未支援會議金鑰(Session Key)封裝與回復(Encapsulation and Recovery)。

5 憑證機構設施、管理及操作控管

5.1 實體控管

5.1.1 所在位置與及結構

HiPKI RCA 機房位於中華電信數據通信分公司，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、入侵偵測及監視錄影等實體安全機制，以防止未經授權存取 HiPKI RCA 之相關設備。

5.1.2 實體存取

HiPKI RCA 以保證等級第 4 級的實體控管規定運作。機房共有四層門禁，第 1 層和第 2 層分別為全年無休的大門及大樓警衛，第 3 層為樓層讀卡機進出管制系統，第 4 層為機房人員指紋辨識進出管制系統，指紋辨識器採用三度空間指紋取樣，可以判別辨識物的紋深、色澤及是否為活體。

除門禁系統可限制不相干人員接近機房外，機箱之監控系統可控制機箱之開啟，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。

任何可攜式儲存媒體帶進機房，需檢查並確認沒有電腦病毒及任何可能危害 HiPKI RCA 系統的惡意軟體。

非 HiPKI RCA 人員進出機房，需填寫進出紀錄，並由 HiPKI RCA 相關人員全程陪同。

HiPKI RCA 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：

(1) 確認設備是否正常運作。

(2) 確認機箱門是否關閉。

(3) 確認門禁系統是否正常運作。

5.1.3 電力及空調

HiPKI RCA 機房的電力系統，除市電外，另設有發電機(滿載油料可連續運轉 6 天)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，可提供至少 6 小時以上備用電力，供儲存庫備援資料。

HiPKI RCA 機房設有恆溫恆濕空調系統，以控制環境的溫度及濕度，使機房保持最佳運作環境。

5.1.4 水災防範

HiPKI RCA 機房設置在基地墊高的建築物第 3 樓層(含)以上，該建築物並有防水閘門和抽水機，且沒有因為水災造成重大損害紀錄。

5.1.5 火災防範及保護

HiPKI RCA 機房具備自動偵測火災預警功能，系統可自動啟動滅火設備，並設置手動開關於各機房主要出入口，以供現場人員於緊急情況時以手動方式啟動。

5.1.6 媒體儲存

稽核紀錄、歸檔和備援資料的儲存媒體於 HiPKI RCA 機房儲存 1 年，1 年後將移到異地備援場所儲存。

5.1.7 廢料處理

第 9.3.1 節所述之 HiPKI RCA 機密資訊，文件資料部分在不需使用時，將經碎紙機處理；磁帶、硬碟、磁碟、磁光碟(MO)及其他形

式的記憶體，在報廢前，將經格式化程序清除儲存的資料，光碟將被實體銷毀。

5.1.8 異地備援

異地備援的地點與 HiPKI RCA 機房距離 30 公里以上。備援的內容包括資料與系統程式，全部資料備份 1 個星期至少執行 1 次，異動資料備份於異動當天執行,異地備援之非技術安全控管與 HiPKI RCA 為相同的安全等級。

5.2 程序控管

HiPKI RCA 經由作業程序控管(Procedural Controls)，以規定執行系統相關作業的各種可信賴角色(Trusted Role)、每項工作的人員需求數及每個角色的識別與鑑別，以確保系統作業程序之安全。

5.2.1 信賴角色

HiPKI RCA 為使執行系統相關作業的責任，能做適當的區隔，以防止某人惡意使用系統而不被察覺，對於每項系統存取作業，明確規定那些信賴角色才能執行此項作業。

HiPKI RCA 共有 7 種不同的信賴角色，分別為管理員(Administrator)、簽發員(Officer)、稽核員(Auditor)、維運員(Operator)、實體安全控管員(Controller)、網路安全專員及防毒防駭專員，每種信賴角色將依照第 5.3 節規定進行人員控管，以防止可能的內部攻擊。1 種信賴角色可由多人擔任，每種信賴角色設有 1 名主管(Chief Role)，7 種信賴角色的工作內容說明如下：

(1) 管理員負責：

- 安裝、設定和維護 HiPKI RCA 系統。
- 建立和維護 HiPKI RCA 系統之使用者帳號。

- 設定稽核參數。
- 產製和備份 HiPKI RCA 之金鑰。
- 公布憑證機構廢止清冊於儲存庫。

(2) 簽發員負責：

- 啟動/停止憑證簽發服務。
- 啟動/停止憑證廢止服務。
- 啟動/停止憑證機構廢止清冊簽發服務。

(3) 稽核員負責：

- 對稽核紀錄的查驗、維護和歸檔。
- 執行或監督內部的稽核，以確認 HiPKI RCA 運作是否遵照本作業基準的規定。

(4) 維運員負責：

- 系統設備的日常運作維護。
- 系統的備援及復原作業。
- 儲存媒體的更新。
- 除 HiPKI RCA 憑證管理系統外之軟硬體更新。
- 網站的維護。
- 建置系統安全與病毒或惡意軟體等威脅之防護機制。

(5) 實體安全控管員負責：

- 系統的實體安全控管(如機房的門禁管理、防火、防水及空調系統等)。

(6) 網路安全專員負責：

- 網路和網路設備的維護。
- 網路設備之弱點修補作業。

- HiPKI RCA 之網路安全。
- 網路安全事件的偵測與通報。

(7) 防毒防駭專員負責：

- 研議、應用或提供防毒防駭、防惡意軟體等威脅之技術或措施，以確保系統和網路之安全。
- 將蒐集之電腦病毒之威脅或弱點通報系統管理員或網路安全專員進行修補。

5.2.2 每項任務所需之人數

依據各種信賴角色的作業安全需求，所需之人數如下：

(1) 管理員：至少 3 位合格人員擔任。

(2) 簽發員：至少 3 位合格人員擔任。

(3) 稽核員：至少 2 位合格人員擔任。

(4) 維運員：至少 2 位合格人員擔任。

(5) 實體安全控管員：至少 2 位合格人員擔任。

(6) 網路安全專員：至少 1 位合格人員擔任。

(7) 防毒防駭專員：至少 1 位合格人員擔任。

每項任務所需之人數說明如下：

任務名稱	管理員	簽發員	稽核員	維運員	實體安全控管員	網路安全專員	防毒防駭專員
安裝、設定和維護 HiPKI RCA 憑證管理系統	2				1		
建立和維護 HiPKI RCA	2				1		

任務名稱	管理員	簽發員	稽核員	維運員	實體安全控管員	網路安全專員	防毒防駭專員
憑證管理系統之使用者帳號							
設定稽核參數	2				1		
產製和備份 HiPKI RCA 之金鑰	2		1		1		
公布憑證機構廢止清冊在儲存庫	1				1		
啟動/停止憑證簽發服務		2			1		
啟動/停止憑證廢止服務		2			1		
啟動/停止憑證機構廢止清冊簽發服務		2			1		
對稽核紀錄的查驗、維護和歸檔			1		1		
系統設備的日常運作維護				1	1		
系統的備援及復原作業				1	1		
儲存媒體的				1	1		

任務名稱	管理員	簽發員	稽核員	維運員	實體安全控管員	網路安全專員	防毒防駭專員
更新							
除 HiPKI RCA 憑證管理系統外之軟硬體更新				1	1		
網站的維護				1	1		
網路和網路設備的日常運作維護				1	1	1	
網路設備之弱點修補作業	1				1	1	
電腦病毒威脅與弱點之通報事項							1
系統病毒碼與弱點之修補作業				1	1		

5.2.3 識別及鑑別每個角色

HiPKI RCA 利用使用者帳號、通行碼和群組之系統帳號管理功能及 IC 卡，識別及鑑別管理員、簽發員、稽核員及維運員等不同角色，並利用中央門禁系統之權限設定功能，識別及鑑別實體安全控管員。HiPKI RCA 利用使用者帳號、通行碼和群組之系統帳號管理功能或其他安全機制識別網路安全專員之角色。

5.2.4 需要職責分離之角色

依照第 5.2.1 節定義的 7 種信賴角色，HiPKI RCA 之角色其職責分離必須符合以下規定：

(1) 管理員、簽發員、稽核員和網路安全專員 4 種信賴角色不得相互兼任，但管理員、簽發員、稽核員可兼任維運員

(2) 實體安全控管員不得兼任管理員、簽發員、稽核員和維運員

(3) 任何 1 種信賴角色均不允許執行自我稽核功能

5.3 人員控管

5.3.1 資格、經驗及清白規定

(1) 人員甄選及進用之安全評估

- 個人性格之評估。
- 申請者經歷之評估。
- 學術、專業能力及資格之評估。
- 人員身分之確認。
- 人員操守之評估。

(2) 人員之考核管理

HiPKI RCA 之相關人員在進用前先進行資格審查，以確認其資格及工作能力。正式進用後，必須接受適當之教育訓練，並以書面方式簽定應負之責任，同時每年進行資格複查，如無法通過資格複查將調離現職，改派其他符合資格人員擔任。

(3) 人員之任免及遷調管理

如人員之進用、約聘僱條件或契約有所變更，特別是人

員離職或約聘僱契約終止時，將遵守維護機密責任之約定。

(4) 維護機密責任之約定

HiPKI RCA 之相關人員均負維護機密之責任，並簽署維護營業秘密契約書，不得以口頭、影印、借閱、交付、文章發表或其他方法洩漏營業秘密。

5.3.2 背景調查程序

HiPKI RCA 對於第 5.2.1 節所述之各種信賴角色人員，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 教育訓練規定

信賴角色	教育訓練規定
管理員	(1) HiPKI RCA 之安全認證機制。 (2) HiPKI RCA 系統安裝、設定和維護之操作程序。 (3) 建立和維護系統交互認證憑證機構帳號之操作程序。 (4) 設定稽核參數之操作程序。 (5) 產製和備份 HiPKI RCA 金鑰之操作程序。 (6) 公布憑證機構廢止清冊於儲存庫之操作程序。 (7) 災後復原及業務永續經營之程序。
簽發員	(1) HiPKI RCA 之安全認證機制。 (2) HiPKI RCA 系統軟硬體的使用及操作程序。 (3) 啟動/停止憑證簽發服務之操作程序。 (4) 啟動/停止憑證廢止服務之操作程序。 (5) 啟動/停止憑證機構廢止清冊簽發服務之操作程序。 (6) 災後復原及業務永續經營之程序。
稽核員	(1) HiPKI RCA 之安全認證機制。

信賴角色	教育訓練規定
	(2) HiPKI RCA 系統軟硬體的使用及操作程序。 (3) 產製和備份 HiPKI RCA 金鑰之操作程序。 (4) 稽核紀錄的查驗、維護和歸檔之程序。 (5) 災後復原及業務永續經營之程序。
維運員	(1) HiPKI RCA 之安全認證機制。 (2) 系統設備日常運作之維護程序。 (3) 儲存媒體之更新程序。 (4) 災後復原以及業務永續經營之程序。 (5) 網站的維護程序。
實體安全控管員	(1) 設定實體門禁權限程序。 (2) 災後復原以及業務永續經營之程序。
網路安全專員	(1) 網路和網路設備的維護程序。 (2) 網路安全機制。
防毒防駭專員	(1) 電腦病毒威脅與弱點及其防制。 (2) 作業系統與網路之安全機制。

5.3.4 人員再教育訓練之頻率及規定

在 HiPKI RCA 之軟硬體升級、工作程序改變、設備更換或相關法規改變時，將安排相關人員再教育訓練並記錄受訓情形，以確實瞭解相關作業程序及法規之改變。

5.3.5 工作輪調之頻率及順序

管理員調離原職務滿 1 年後，才可轉任簽發員或稽核員。

簽發員調離原職務滿 1 年後，才可轉任管理員或稽核員。

稽核員調離原職務滿 1 年後，才可轉任管理員或簽發員。

擔任維運員滿 2 年，且已接受相關教育訓練及通過審核，才可轉

任管理員、簽發員及稽核員。

擔任網路安全專員滿 2 年，且已接受相關教育訓練及通過審核，才可轉任管理員、簽發員及稽核員。

擔任防毒防駭專員滿 2 年，且已接受相關教育訓練及通過審核，才可轉任管理員、簽發員及稽核員。

5.3.6 未授權行為之裁罰

HiPKI RCA 之相關人員，如違反憑證政策與本作業基準或其他 HiPKI RCA 公布之程序，將接受適當的管理與懲處，如情節重大而造成損害者，將採取法律行動追究其責任。

5.3.7 承攬商派駐人員之規定

承攬商派駐人員若擔任信賴角色，其職責、未授權行為之裁罰及應提供之教育訓練文件遵照第 5.3 節規定；操作行為之稽核與監控及相關紀錄保存遵照第 5.4.1 節規定。

5.3.8 提供之文件

HiPKI RCA 提供 HiPKI 憑證政策、技術規範、本作業基準、系統操作手冊及電子簽章法等相關文件給 HiPKI RCA 之相關人員。

5.4 稽核紀錄程序

HiPKI RCA 之安全相關事件，均具有安全稽核紀錄(Audit Log)。安全稽核紀錄採系統自動產生、工作記錄本及紙張等方式。所有安全稽核紀錄均妥善保存，且在執行稽核時可立即取得。安全稽核紀錄之維護依照第 5.5.2 節歸檔之保留期限規定辦理。

5.4.1 被記錄事件種類

(1) 安全稽核

- 任何重要稽核參數之改變，如稽核頻率、稽核事件型態、新舊參數的內容等
- 任何嘗試刪除或修改稽核紀錄檔

(2) 識別與鑑別

- 嘗試新角色的設定不論成功或失敗
- 身分鑑別嘗試的最高容忍次數改變
- 使用者登入系統時身分鑑別嘗試的失敗次數之最大值
- 如管理者將已被鎖住的帳號解鎖，而且該帳號是因為多次失敗的身分鑑別嘗試而被鎖住的
- 管理者改變系統的身分鑑別機制，例如從通行密碼改為生物特徵值

(3) 金鑰產製

- HiPKI RCA 產製金鑰時

(4) 私密金鑰之載入和儲存

- 載入私密金鑰到系統元件中
- 所有為進行金鑰回復工作，對保存在憑證機構的憑證主體之私密金鑰所做的存取

(5) 可信賴公開金鑰之新增、刪除及儲存

- 可信賴公開金鑰之改變，包括新增、刪除及儲存

(6) 私密金鑰之輸出

- 私密金鑰之輸出(不包括只用在單次或只限一次使用之金鑰)

(7) 憑證之註冊

- 憑證之註冊申請過程

(8) 廢止憑證

- 憑證之廢止申請過程

(9) 憑證狀態改變之核可

- 核可或拒絕憑證狀態改變之申請

(10)HiPKI RCA 組態設定

- HiPKI RCA 安全相關之組態設定改變

(11)帳號之管理

- 加入或刪除角色和使用者。
- 使用者帳號或角色之存取權限修改。

(12)憑證格式剖繪之管理

- 憑證格式剖繪之改變。

(13)憑證機構廢止清冊格式剖繪之管理

- 憑證機構廢止清冊格式剖繪之改變。

(14)其他

- 安裝作業系統
- 安裝 HiPKI RCA 系統
- 安裝硬體密碼模組
- 移除硬體密碼模組
- 銷毀硬體密碼模組
- 啟動系統
- 嘗試登入 HiPKI RCA 的憑證管理作業
- 硬體及軟體之接收
- 嘗試設定通行碼

- 嘗試修改通行碼
- HiPKI RCA 之內部資料備份
- HiPKI RCA 之內部資料回復
- 檔案操作(例如產生、重新命名及移動等)
- 傳送任何資訊到儲存庫公布
- 存取 HiPKI RCA 之內部資料庫
- 任何憑證被破解之申告
- 憑證載入符記
- 符記之傳遞過程
- 符記之零值化
- HiPKI RCA 或交互認證憑證機構之金鑰更換。

(15)HiPKI RCA 之伺服器設定改變

- 硬體
- 軟體
- 作業系統
- 修補程式 (Patches)
- 安全格式剖繪

(16)實體存取及場所之安全

- 人員進出 HiPKI RCA 之機房
- 存取 HiPKI RCA 之伺服器
- 得知或懷疑違反實體安全規定

(17)異常

- 軟體錯誤
- 軟體檢查完整性失敗
- 接收不合適訊息

- 非正常路由之訊息
- 網路攻擊(懷疑或確定)
- 設備失效
- 電力不當
- 不斷電系統(UPS) 失敗
- 明顯及重大的網路服務或存取失敗
- 憑證政策之違反
- 本作業基準之違反
- 重設系統時鐘

5.4.2 紀錄檔處理頻率

HiPKI RCA 每月檢視 1 次稽核紀錄，追蹤調查重大事件。檢視工作包括驗證稽核紀錄是否被竄改、檢視所有的紀錄項目及檢查任何警示或異常等。HiPKI RCA 自上次稽核檢視後所發生的重大安全稽核紀錄都應加以檢視，並且對任何可能之惡意活動應進一步調查。檢視稽核紀錄之結果以文件記錄。

5.4.3 稽核紀錄檔保留期限

稽核紀錄檔現場(on site)保留兩個月，再移至適當場所儲存，並依照第 5.5.2 節稽核記錄保留期限之相關規定辦理。

憑證機構應確保稽核紀錄檔可於合格稽核業者執行外部稽核時取得。當稽核紀錄檔的保留期限屆滿，如須移除該資料，必須由稽核員移除，不可由其他人員代理。

5.4.4 稽核紀錄檔之保護

使用簽章、加密技術保存目前和已歸檔之稽核紀錄，並使用 CD-R 或其他無法更改稽核紀錄的媒體儲存。

簽署事件紀錄的私密金鑰不能再使用於其他用途，嚴禁稽核系統之私密金鑰另作他用，稽核系統不可洩漏私密金鑰。

手動的稽核紀錄存放於安全場所。

5.4.5 稽核紀錄檔備份程序

電子式稽核紀錄每月備份及異地(off-site)備援 1 次。

HiPKI RCA 週期性地將事件紀錄備份：稽核系統將稽核軌跡資料以每日、每星期及每月等條件週期性地自動歸檔。

HiPKI RCA 將事件紀錄檔存放於安全場所。

5.4.6 稽核彙整系統

稽核系統內建於憑證管理系統。稽核紀錄程序應在憑證管理系統啟動時啟用，唯有在憑證管理系統關閉時才停止。

如自動稽核系統無法正常運作，同時保護系統資料之完整性、機密性的安全機制處於高風險狀態時，HiPKI RCA 將暫停憑證簽發服務，直到問題解決後再行提供服務。

5.4.7 對引起事件者之通知

不做規定。

5.4.8 弱點評估

HiPKI RCA 遵照 WebTrust for CA－SSL BR 及 Network and Certificate System Security Requirements 規定之方式與頻率每季執行弱點評估至少 1 次，每年執行滲透測試至少 1 次。HiPKI RCA 於認定應用程式或基礎設施(Infrastructure)重大更新或變更後，也須執行滲透測試。HiPKI RCA 於滲透測試與弱點評估後進行補強與矯正措施。HiPKI RCA 針對足以執行可信賴的弱點掃瞄、滲透測試、資安健診或

安全監控之人員或團體，記錄其技能、工具、遵循之道德倫理規範、競業關係以及獨立性。

5.5 紀錄歸檔

5.5.1 歸檔紀錄之種類

- HiPKI RCA 被主管機關認證(Accreditation)的資料(假設適用)。
- 憑證實務作業基準。
- 交互認證協議書(假設適用)。
- 系統與設備組態設定。
- 系統或組態設定修改與更新的內容。
- 憑證申請資料。
- 憑證廢止資料。
- 憑證接受的確認文件。
- 已簽發或公告的憑證。
- HiPKI RCA 金鑰更換的紀錄。
- 已簽發或公告的憑證機構廢止清冊。
- 稽核記錄。
- 用來驗證及佐證歸檔內容的其它說明資料或應用程式。
- 稽核人員要求的文件。
- 組織身分及個人身分鑑別資料。

5.5.2 歸檔資料保留期限

HiPKI RCA 歸檔資料之保留期限為 20 年，用來處理歸檔資料的應用程式也將維護 20 年。

歸檔資料逾保留期限後，書面資料應以安全方式銷毀；電子形式資料備份得另備份至其他儲存媒體並提供適當保護，或逕行以安全方

式銷毀。

5.5.3 歸檔資料之保護

不允許新增、修改或刪除歸檔資料。

HiPKI RCA 可將歸檔資料移到另一個儲存媒體，並提供適當的保護，保護等級不低於原保護等級。

歸檔資料存放於安全場所。

5.5.4 歸檔資料備份程序

歸檔資料備份至異地備援中心，異地備援的地點參閱第 5.1.8 節。

5.5.5 記錄之時戳規定

歸檔之電子式紀錄(例如憑證、憑證機構廢止清冊及稽核紀錄等)包含日期與時間資訊，而且這些紀錄皆經過適當的數位簽章保護，可用以檢測紀錄中的日期與時間資訊是否遭到篡改。但是，這些電子式紀錄中的日期與時間資訊並非公正第三者所提供之電子式時戳資料，而是電腦作業系統的日期與時間。HiPKI RCA 的所有電腦系統都會定期進行校時，以確保電子式紀錄中日期與時間資訊的準確性與可信度。

歸檔的書面紀錄也將記載日期資訊，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人員簽名確認。

5.5.6 歸檔資料彙整系統

HiPKI RCA 沒有歸檔資料彙整系統。

5.5.7 取得及驗證歸檔資料之程序

必須以書面申請獲得正式授權後，才可取得歸檔資料。

由稽核員負責驗證歸檔資料，書面文件必須驗證文件簽署者及日期等之真偽，電子檔則驗證歸檔資料的數位簽章。

5.6 HiPKI RCA 之金鑰更換

HiPKI RCA 在以下兩種情形會更換金鑰並簽發新的自簽憑證：

(1) 目前使用之金鑰生命週期結束

(2) 目前使用之金鑰的安全性有問題時(例如懷疑或確定金鑰被破解)

HiPKI RCA 之私密金鑰應依照第 6.3.2.1 節規定定期更換，HiPKI RCA 最遲應於其私密金鑰簽發憑證機構憑證的使用期限到期前，更換金鑰對。HiPKI RCA 更換金鑰對後，應以新私密金鑰簽發 1 張新的自簽憑證及使用新舊私密金鑰相互簽發 1 張新自發憑證，此 3 張新憑證的簽發程序依照第 4.3 節規定。新簽發的自簽憑證依照第 6.1.4 節規定傳送給信賴憑證者，自發憑證公布在儲存庫供信賴憑證者下載。

5.7 破解及災變之復原

5.7.1 緊急事件及系統遭破解之處理程序

HiPKI RCA 訂定緊急事件及系統遭破解後之通報與處理程序，同時每年進行演練。

5.7.2 電腦資源、軟體或資料遭破壞

HiPKI RCA 訂定電腦資源、軟體或資料遭破壞之復原程序，同時每年進行演練。

如 HiPKI RCA 的電腦設備遭破壞或無法運作，但 HiPKI RCA 的簽章金鑰並未被損毀，則優先回復 HiPKI RCA 儲存庫之運作，使憑證狀態資訊能正常提供。

5.7.3 HiPKI RCA 私密金鑰遭破解之處理程序

HiPKI RCA 訂定簽章金鑰遭破解之復原程序，以迅速恢復憑證之簽發及管理作業能力，同時每年進行演練。

5.7.4 災變後業務持續營運能力

HiPKI RCA 每年對其災後復原計畫進行演練。

5.8 HiPKI RCA 之終止服務

HiPKI RCA 終止服務時，將依據電子簽章法相關規定辦理。

HiPKI RCA 遵守以下事項，以確保終止服務對於下屬憑證機構、交互認證憑證機構與信賴憑證者造成之影響最小：

(1) HiPKI RCA 於預定終止服務 3 個月前，將通知下屬憑證機構、交互認證憑證機構(無法通知者，不在此限)與將 HiPKI RCA 自簽憑證植入根憑證機構信賴清單的應用軟體供應商(如瀏覽器或作業系統廠商)，並公告於儲存庫。

(2) HiPKI RCA 終止服務時，廢止所有未廢止及未過期之憑證，並依電子簽章法相關規定進行檔案紀錄之保管及移交。

6 技術性安全控管

6.1 金鑰對之產製及安裝

6.1.1 金鑰對之產製

HiPKI RCA 依照第 6.2.1 節規定，於硬體密碼模組內產製金鑰對，依照 NIST FIPS 140-2 規範之演算法，私密金鑰之匯出與匯入依照第 6.2.2 與第 6.2.6 節規定辦理。

HiPKI RCA 之金鑰產製由相關人員見證及錄影留存，並簽署金鑰啟用見證書(其中記載產製的金鑰對之公開金鑰)，並透過公信管道公布 HiPKI RCA 金鑰對之公開金鑰，以昭公信。其中，相關人員應包含政策管理委員會之委員及合格稽核業者(Qualified Auditor)。

下屬憑證機構與交互認證之憑證機構必須依照憑證政策之規定進行金鑰對之產製。

HiPKI RCA 在簽發下屬憑證機構與交互認證憑證機構之憑證時，將檢查憑證申請檔中之公開金鑰，確定該憑證機構的公開金鑰在 HiPKI RCA 所簽發過的憑證中是唯一的。

HiPKI RCA 使用硬體密碼模組產製亂數、公開金鑰對和對稱金鑰。

下屬憑證機構必須依照憑證政策之規定，選擇適當的軟體或硬體進行金鑰產製；HiPKI RCA 於簽發下屬憑證機構憑證前將審查該下屬憑證機構所選擇的軟體或硬體是否恰當。

交互認證之憑證機構必須依照憑證政策之規定，選擇適當的軟體或硬體進行金鑰產製；HiPKI RCA 於簽發交互憑證前將審查該憑證機構所選擇的軟體或硬體是否恰當。

HiPKI RCA 僅提供自簽憑證、自發憑證、下屬憑證機構憑證與交互憑證之簽發，未提供用戶憑證之簽發。有關於用戶憑證金鑰對產製之相關規定請參閱本基礎建設之下屬憑證機構的憑證實務作業基準或交互認證機構之憑證實務作業基準。

6.1.2 私密金鑰傳送給憑證機構

下屬憑證機構必須自行產製私密金鑰，因此 HiPKI RCA 不需將私密金鑰傳送給下屬憑證機構。

與 HiPKI RCA 交互認證的根憑證機構必須自行產製私密金鑰，因此 HiPKI RCA 不需將私密金鑰傳送給交互認證憑證機構。

6.1.3 公開金鑰傳送給簽發憑證機構

由憑證機構於申請憑證時提交 PKCS#10 的憑證申請檔。

6.1.4 憑證機構公開金鑰傳送給信賴憑證者

HiPKI RCA 本身之自簽憑證內含 HiPKI RCA 之公開金鑰，安全散布管道包括以下幾種：

(1) HiPKI RCA 金鑰產製時，當場公布 HiPKI RCA 之公開金鑰，並由政策管理委員會委員與合格稽核業者簽署 HiPKI RCA 公開金鑰見證書，於 HiPKI RCA 簽發自簽憑證後公布於 HiPKI RCA 網站儲存庫。

(2) HiPKI RCA 在簽發下屬憑證機構憑證給下屬憑證機構後，於遞交下屬憑證機構憑證時，一併將 HiPKI RCA 之自簽憑證或公開金鑰遞交給該下屬憑證機構，該下屬憑證機構以符記(例如 IC 卡)儲存 HiPKI RCA 之自簽憑證或公開金鑰，並以安全方式傳送給該下屬憑證機構的用戶或信賴憑證者。

(3) HiPKI RCA 在簽發交互憑證給交互認證憑證機構後，於遞交交互憑證時，一併將 HiPKI RCA 之自簽憑證或公開金鑰遞交給該交互認證憑證機構，該交互認證憑證機構以符記(例如 IC 卡)儲存 HiPKI RCA 之自簽憑證或公開金鑰，並以安全方式傳送給該交互認證憑證機構的用戶或信賴憑證者。

(4) 將 HiPKI RCA 本身之自簽憑證存至(Build-in)可信賴之第三者所發行的軟體中，用戶透過安全管道取得軟體(例如向可信賴的經銷商購買軟體的安裝光碟或是透過各大作業系統或瀏覽器之安裝)並安裝後，便可得到 HiPKI RCA 之自簽憑證。

(5) 在大量發行的光碟中放置 HiPKI RCA 之自簽憑證，用戶透過安全管道取得這些光碟，便可得到 HiPKI RCA 之自簽憑證。

6.1.5 金鑰長度

HiPKI RCA、下屬憑證機構及交互認證憑證機構用於簽發憑證、憑證機構廢止清冊及憑證廢止清冊之金鑰及演算法須滿足下述規定：

(1) HiPKI RCA

- 使用金鑰長度為 4096 位元的 RSA 金鑰及 SHA-256、SHA-384 或 SHA-512 雜湊函數演算法簽發憑證。
- 未來若使用橢圓曲線密碼演算法(Elliptic Curve Cryptography, ECC)簽發憑證，則使用符合 NIST P-384 之金鑰長度。

(2) 下屬憑證機構與交互認證憑證機構

- 依憑證政策之規定，使用金鑰長度為 4096 位元的 RSA 金鑰及 SHA-256、SHA-384 或 SHA-512 雜湊函數演算法簽發憑證。

■ 未來若使用橢圓曲線密碼演算法簽發憑證，則使用符合 NIST P-256 或 P-384 之金鑰長度。

HiPKI RCA 於簽發下屬憑證機構憑證與交互憑證前，將審查該憑證機構所選擇的金鑰長度是否恰當。

6.1.6 公開金鑰參數之產製及品質檢驗

採用 RSA 演算法之公開金鑰參數為空的(Null)。

HiPKI RCA 與下屬憑證機構採用 ANSI X9.31 演算法或 NIST FIPS 186-4 規範產生 RSA 演算法所需的質數，並保證該質數為強質數(Strong Prime)。

交互認證之憑證機構必須依據所選用的演算法，進行適當的金鑰參數品質檢驗。

根據 NIST SP 800-89 第 5.3.3 節，HiPKI RCA 確認公鑰指數(Public Exponent)的值為大於 3 的奇數，且其值介於 $2^{16}+1$ 與 $2^{256}-1$ 之間。此外，模數(Modulus)具有奇數、非質數的指數次方且沒有小於 752 的因數等性質。

未來若使用橢圓曲線密碼演算法簽發憑證，HiPKI RCA 將遵循 NIST SP 800-56A Revision 2 第 5.6.2.3.2 節與第 5.6.2.3.3 節之規定，確認所有使用 ECC Full Public Key Validation Routine 與 ECC Partial Public Key Validation Routine 的金鑰之效期。

6.1.7 金鑰之使用目的

HiPKI RCA 之自簽憑證相對應的私密金鑰僅限用於簽發自簽憑證、自發憑證、下屬憑證機構憑證、交互憑證、憑證機構廢止清冊、以及線上憑證狀態協定回應伺服器憑證或線上憑證狀態協定回應訊

息。

HiPKI RCA 自簽憑證包含金鑰用途擴充欄位，且標示為關鍵性(Critical)欄位，其金鑰用途位元預設為 keyCertSign 與 cRLSign。若 HiPKI RCA 欲使用其簽章用私密金鑰簽發線上憑證狀態協定回應訊息時，則金鑰用途位元尚須包含 digitalSignature。

HiPKI RCA 簽發給下屬憑證機構的憑證，其金鑰用途擴充欄位設定使用的金鑰用途位元為 keyCertSign 與 cRLSign。若該下屬憑證機構欲使用其簽章用私密金鑰簽發線上憑證狀態協定回應訊息時，則金鑰用途位元尚須包含 digitalSignature。

HiPKI RCA 簽發給交互認證憑證機構的憑證，其金鑰用途擴充欄位設定使用的金鑰用途位元為 keyCertSign 與 cRLSign。若該交互認證憑證機構欲使用其簽章用私密金鑰簽發線上憑證狀態協定回應訊息時，則金鑰用途位元尚須包含 digitalSignature。

6.2 私密金鑰保護及密碼模組工程控管

6.2.1 密碼模組標準及控管

HiPKI RCA 依據憑證政策的規定，使用符合 FIPS 140-2 安全等級 3 的硬體密碼模組。

下屬憑證機構必須依照憑證政策之規定，選擇適當的密碼模組；HiPKI RCA 於簽發下屬憑證機構憑證前將審查該憑證機構所選擇的密碼模組之安全等級是否恰當。

交互認證之憑證機構必須依照憑證政策之規定，選擇適當的密碼模組；HiPKI RCA 於簽發交互憑證前將審查該憑證機構所選擇的密碼模組之安全等級是否恰當。

6.2.2 私密金鑰分持之多人控管

HiPKI RCA 金鑰分持之多人控管，採 LaGrange 多項式內插法(LaGrange Polynomial Interpolation)的 n-out-of-m (簡稱 n-out-of-m)，他是一種完全秘密分享(Perfect Secret Sharing)的方式，可做為私密金鑰分持備份及回復方法；其中，n 與 m 皆須為大於或等於 2 的數值，且 n 必須小於或等於 m。採用此方法可使 HiPKI RCA 私密金鑰的多人控管具有最高的安全度，因此也用來做為私密金鑰之啟動方式(參閱第 6.2.8 節)。

如為欲簽發保證等級第 3 及第 4 級憑證的憑證機構之簽章用私密金鑰，必須依據憑證政策規定採用多人控管程序。HiPKI RCA 於簽發下屬憑證機構憑證或交互憑證前將審查該憑證機構所採用的多人控管程序是否恰當。

6.2.3 私密金鑰託管

HiPKI RCA 簽章用私密金鑰不可被託管，HiPKI RCA 也不負責保管下屬憑證機構與交互認證憑證機構的簽章用私密金鑰。

6.2.4 私密金鑰備份

依照 6.2.2 節的金鑰分持之多人控管方法備份私密金鑰，並使用高安全性的 IC 卡做為秘密分持的儲存媒體。

下屬憑證機構與交互認證之憑證機構必須依照憑證政策之規定，選擇適當的私密金鑰備份方法；HiPKI RCA 於簽發下屬憑證機構與交互憑證前將審查該憑證機構所選擇的私密金鑰備份方法是否恰當。

HiPKI RCA 不負責保管下屬憑證機構與交互認證憑證機構的私密金鑰備份。

6.2.5 私密金鑰歸檔

HiPKI RCA 簽章用私密金鑰不可被歸檔，但其相對應的公開金鑰會依第 5.5 節之規定，以憑證檔案格式進行歸檔。HiPKI RCA 不對下屬憑證機構與交互認證憑證機構簽章用私密金鑰進行歸檔。

6.2.6 私密金鑰匯入、匯出密碼模組

私密金鑰僅於金鑰備份、金鑰回復或更換密碼模組時，始可從密碼模組匯出並匯入至備份專用之符記，其過程應遵循第 6.2.2 節規定多人控管方式。私密金鑰從密碼模組匯出或於密碼模組間傳輸時需使用加密或金鑰分持等方式保護，以確保私密金鑰不曾以明碼呈現。私密金鑰輸入完成後，須將輸入過程產製之相關機密參數完全銷毀。

下屬憑證機構與交互認證之憑證機構如需將私密金鑰輸入密碼模組，必須依照憑證政策之規定，選擇適當的私密金鑰輸入方法；HiPKI RCA 於簽發下屬憑證機構或交互憑證前將審查該憑證機構所選擇的私密金鑰輸入方法是否恰當。

若 HiPKI RCA 發現下屬憑證機構或交互認證之憑證機構之私密金鑰洩漏給未授權人員或不屬於該憑證機構之組織的情形，HiPKI RCA 將廢止與該憑證機構之私密金鑰相關之憑證。

6.2.7 私密金鑰儲存於密碼模組

依照第 6.1.1 節及第 6.2.1 節規定。

6.2.8 啟動私密金鑰之方式

HiPKI RCA 之 RSA 私密金鑰之啟動(Activation)，是以多人控管 IC 卡進行控制，不同用途的控管 IC 卡分別由管理員及簽發員保管。

下屬憑證機構與交互認證之憑證機構必須依照憑證政策之規定，選擇適當的私密金鑰啟動方式；HiPKI RCA 於簽發下屬憑證機構與交互憑證前將審查該憑證機構所選擇的私密金鑰啟動方式是否恰當。

6.2.9 停用私密金鑰之方式

由於 HiPKI RCA 採離線作業方式，因此平常 HiPKI RCA 之金鑰對保持在停用(Deactivation)狀態，以避免私密金鑰遭非法使用。

每次完成簽發憑證及相關管理作業後，將採多人控管方式將私密金鑰停用。下屬憑證機構與交互認證之憑證機構必須依照憑證政策之規定，選擇適當的私密金鑰停用方式；HiPKI RCA 於簽發下屬憑證機構與交互憑證前將審查該憑證機構所選擇的私密金鑰停用方式是否恰當。

6.2.10 銷毀私密金鑰之方式

為避免 HiPKI RCA 舊的私密金鑰被盜用，影響簽發憑證之正確性，HiPKI RCA 之私密金鑰生命週期屆滿時將加以銷毀。因此，在 HiPKI RCA 完成金鑰更新及簽發新的 HiPKI RCA 自簽憑證，且不再簽發任何憑證與憑證機構廢止清冊之後，將會把硬體密碼模組中存放舊的 HiPKI RCA 私密金鑰之記憶位置填零(Zeroization)，以銷毀硬體密碼模組中舊的私密金鑰。同時，舊的私密金鑰之分持也將進行實體銷毀。

倘若硬體密碼模組將不再提供 HiPKI RCA 所需之服務，但其仍可被存取時，則此硬體密碼模組中所有的私密金鑰(包含曾經使用過或是可能被使用的私密金鑰)皆應被銷毀。在銷毀該硬體密碼模組中

的私密金鑰後，須再使用該硬體密碼模組所提供的金鑰管理工具加以檢視，確認前述所有私密金鑰已確實不存在。

下屬憑證機構與交互認證之憑證機構必須依照憑證政策之規定，選擇適當的私密金鑰銷毀方式；HiPKI RCA 於簽發下屬憑證機構與交互憑證前將審查該憑證機構所選擇的私密金鑰銷毀方式是否恰當。

6.2.11 密碼模組評等

參見第 6.2.1 節。

6.3 金鑰對管理之其他規範

下屬憑證機構與交互認證憑證機構必須自行管理金鑰對，HiPKI RCA 不負責保管下屬憑證機構與交互認證憑證機構的私密金鑰。

6.3.1 公開金鑰歸檔

HiPKI RCA 將進行憑證之歸檔，且依照第 5.5 節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，因憑證之歸檔可代替公開金鑰之歸檔。

6.3.2 憑證操作及金鑰對之使用期限

HiPKI RCA 僅提供自簽憑證、自發憑證、下屬憑證機構憑證、交互憑證、憑證機構廢止清冊以及線上憑證狀態協定回應伺服器憑證或線上憑證狀態協定回應訊息之簽發，未提供用戶憑證之簽發。有關於簽發用戶憑證之相關規定請參閱本基礎建設之下屬憑證機構的憑證實務作業基準或交互認證機構之憑證實務作業基準。

6.3.2.1 HiPKI RCA 憑證操作及金鑰對之使用期限

HiPKI RCA 公開金鑰及私密金鑰之金鑰長度為 RSA 4096 位元，使用期限至多為 30 年；以私密金鑰執行簽發下屬憑證機構憑證或交互憑證之用途使用期限至多為 15 年，但用於簽發憑證機構廢止清冊、線上憑證狀態協定回應伺服器憑證或線上憑證狀態協定回應訊息之用途時，則使用至 HiPKI RCA 所簽發之下屬憑證機構憑證、自發憑證或交互憑證效期到期為止，復因異動憑證政策也可能有需要重新簽發自發憑證，故 HiPKI RCA 之私密金鑰用於簽發自發憑證之使用期限至多 30 年。

線上憑證狀態協定回應伺服器之私密金鑰與公鑰憑證使用期限為 36 小時，每天會公布新的線上憑證狀態協定回應伺服器憑證(透過新私密金鑰進行數位簽章的線上憑證狀態協定回應訊息包含該憑證，以供信賴憑證者驗證線上憑證狀態協定回應訊息之簽章)。

HiPKI RCA 本身之自簽憑證效期應考量涵蓋與憑證之公開金鑰相對應之私密金鑰簽發的所有憑證效期到期為止。

HiPKI RCA 新舊金鑰互簽之自發憑證之效期應至 HiPKI RCA 舊金鑰簽發之自簽憑證效期到期為止。

6.3.2.2 下屬憑證機構與交互認證憑證機構憑證操作及金鑰對之使用期限

下屬憑證機構與交互認證憑證機構之公開金鑰及私密金鑰長度為 RSA 4096 位元，使用期限至多為 20 年；以私密金鑰執行簽發用戶憑證之用途，其使用期限至多為 10 年，但簽發憑證廢止清冊、線上憑證狀態協定回應伺服器憑證或線上憑證狀態協定回應訊息之用途則不在此限。

HiPKI RCA 簽發之下屬憑證機構憑證或交互憑證之效期不得超過 HiPKI RCA 自簽憑證之效期。

6.3.2.3 雜湊函數演算法有效期限

HiPKI RCA 使用 SHA-256 雜湊函數演算法簽發自簽憑證、自發憑證、下屬憑證機構憑證、交互憑證及憑證機構廢止清冊。

HiPKI RCA 線上憑證狀態協定回應伺服器採 RSA 2048 併同 SHA-256 演算法簽發線上憑證狀態協定回應訊息。

本基礎建設之下屬憑證機構或與本基礎建設交互認證之憑證機構應採用 SHA-256 或更高安全等級之雜湊函數演算法簽發用戶憑證、憑證廢止清冊及線上憑證狀態協定回應訊息。

6.4 啟動資料

6.4.1 啟動資料之產生及安裝

HiPKI RCA 之啟動資料由硬體密碼模組產生，再寫入 n-out-of-m 控管 IC 卡中。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 卡的個人識別碼(Personal Identification Number，簡稱 PIN 碼)直接在硬體密碼模組內建的鍵盤上輸入。

下屬憑證機構與交互認證之憑證機構必須依照憑證政策之規定，選擇適當的啟動資料產生方式；HiPKI RCA 於簽發下屬憑證機構與交互憑證前將審查該憑證機構所選擇的啟動資料產生方式是否恰當。

6.4.2 啟動資料之保護

HiPKI RCA 之啟動資料由 n-out-of-m 控管 IC 卡保護，IC 卡的 PIN 碼由保管人員負責保存，不得記錄於任何媒體上，如登入的失敗次數

超過 3 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。

下屬憑證機構與交互認證之憑證機構必須依照憑證政策之規定，選擇適當的啟動資料保護方式；HiPKI RCA 於簽發下屬憑證機構憑證與交互憑證前將審查該憑證機構所選擇的啟動資料保護方式是否恰當。

6.4.3 啟動資料之其他規範

HiPKI RCA 的私密金鑰的啟動資料不做歸檔。

6.5 電腦安全控管

6.5.1 特定電腦安全技術規定

HiPKI RCA 和相關輔助系統透過作業系統，或結合作業系統、軟體和實體的保護措施提供以下安全控管功能：

- 具備身分鑑別之登入
- 依所擔任之角色定義存取權限
- 提供安全稽核能力
- 以密碼技術確保每次通訊和資料庫之安全
- 具備程序完整性及安全控管保護

HiPKI RCA 設備建構在經過安全評估的作業平臺上，且硬體、軟體、作業系統在經過安全評估的組態下運作，對能夠導致簽發憑證之帳號實施多因子認證。

6.5.2 電腦安全評等

憑證中心憑證伺服器採用通過 Common Criteria EAL 4 認證的電腦作業系統。

6.6 生命週期技術控管

6.6.1 系統研發控管

HiPKI RCA 的系統研發遵循 CMMI 的規範進行品質控管。

系統開發環境、測試環境及上線運作環境必須有所區隔防止未經授權存取或變更的風險。

各項交付 HiPKI RCA 之產品或程式應簽署安全遵循保證書確保無後門或惡意程式，並提供產品或程式交付清單、測試報告、系統管理手冊及原始程式碼掃瞄報告等，並進行程式版本控管。

6.6.2 安全管理控管

HiPKI RCA 之硬體與軟體是專用的，僅能使用獲得安全授權的元件，不安裝與運作無關的硬體裝置、網路連接或元件軟體，並且在每次使用時會檢查是否有惡意程式碼。

HiPKI RCA 的軟體在首次安裝時，將確認是由供應商提供正確的版本且未被修改。系統安裝後，HiPKI RCA 於每次使用時檢驗軟體的完整性，並定期使用防毒軟體與惡意軟體移除工具進行掃瞄。

HiPKI RCA 將記錄與控管系統的組態及任何修正與功能提升，同時偵測未經許可修改系統之軟體或組態。

HiPKI RCA 在風險評鑑、風險處理及安全管理控管措施參考 ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 27005、ISO/IEC 31000、WebTrust for CA 及 Baseline Requirements 之方法論或控制項。

6.6.3 生命週期安全控管

每年至少 1 次評估現行金鑰是否有被破解之風險。

6.7 網路安全控管

HiPKI RCA 之主機不與外部網路連接，儲存庫連接到網際網路(Internet)上，提供不中斷之憑證及憑證機構廢止清冊查詢服務(除必要之維護或備援外)。

HiPKI RCA 主機所簽發之憑證及憑證機構廢止清冊以數位簽章保護，使用手動方式，從 HiPKI RCA 主機傳送到儲存庫。

HiPKI RCA 之儲存庫透過系統修補程式的更新、系統弱點掃描、入侵防禦系統/入侵偵測系統、防火牆系統及過濾路由器(Filtering Router)等加以保護，以防範阻絕服務及入侵等攻擊。

6.8 時戳

HiPKI RCA 定期根據受信賴的時間源進行系統校時，以維持系統時間的正確性，並確保以下時間之正確性：

(1) 憑證簽發時間

(2) 憑證廢止時間

(3) 憑證機構廢止清冊之簽發時間

(4) 系統事件之發生時間

HiPKI RCA 可能會使用自動與手動程序來進行系統時間調整，系統校時動作需可被稽核。

7 憑證、憑證廢止清冊及線上憑證狀態協定之格式剖繪

7.1 憑證之格式剖繪

HiPKI RCA 所簽發的憑證遵循 ITU-T X.509、Baseline Requirements 及 RFC 5280 之規定。

HiPKI RCA 透過密碼學安全偽亂數生成器(Cryptographically Secure Pseudorandom Number Generator, CSPRNG)產生其所簽發之憑證的憑證序號，此憑證序號為長度至少 64 位元且非循序之正整數。

7.1.1 版本序號

HiPKI RCA 簽發遵循 RFC 5280 與 ITU-T 規範之 X.509 v3 憑證。

7.1.2 憑證擴充欄位

HiPKI RCA 簽發的憑證之憑證擴充欄位遵循 ITU-T X.509、Baseline Requirements 及 RFC 5280 之規定。

HiPKI RCA 簽發的憑證有 4 種，分別為自簽憑證、自發憑證、下屬憑證機構憑證及交互憑證，其所使用之必要擴充欄位以及該擴充欄位的關鍵性(Critical)與內容如下所述。其他選擇性擴充欄位依情況不同使用之，使用方式遵循前述標準之規定。

(1) 自簽憑證

擴充欄位	關鍵性	內容
主體金鑰識別碼 (Subject Key Identifier)	FALSE	主體(Subject)的公開金鑰 SHA-1 雜湊值

基本限制 (Basic Constraints)	TRUE	Subject Type=CA Path Length Constraint=None
金鑰用途 (Key Usage)	TRUE	此擴充欄位內容可為下述其中一種： ■ keyCertSign 與 cRLSign(預設) ■ digitalSignature、keyCertSign 及 cRLSign(若 HiPKI RCA 欲使用其簽章用私密金鑰簽發線上憑證狀態協定回應訊息時，則須再包含 digitalSignature)

(2) 自發憑證

擴充欄位	關鍵性	內容
憑證機構金鑰識別碼 (Authority Key Identifier)	FALSE	簽發者(Issuer)的公開金鑰 SHA-1 雜湊值
主體金鑰識別碼 (Subject Key Identifier)	FALSE	主體(Subject)的公開金鑰 SHA-1 雜湊值
CRL 發布點 (CRL Distribution Points)	FALSE	HiPKI RCA 公告之憑證機構廢止清冊的網址
憑證機構資訊存取 (Authority Information Access)	FALSE	此擴充欄位包含以下兩項資訊： ■ HiPKI RCA 之自簽憑證下載網址 ■ HiPKI RCA 所提供之線上憑證狀態協定查詢服務的網址
憑證政策 (Certificate Policies)	FALSE	此擴充欄位須包含以下兩項資訊，並可視憑證需求使用政策限定元(Policy Qualifiers)，用於標示本作業基準公告之網址： ■ 本基礎建設憑證政策定義之所有憑證政策物件識別碼 ■ 本基礎建設憑證政策引用之所有 CA/Browser Forum 定義之憑證政策物件識別碼。
金鑰用途 (Key Usage)	TRUE	此擴充欄位內容應與簽發此憑證之 HiPKI RCA 自簽憑證之金鑰用途擴充欄位相同。
基本限制 (Basic Constraints)	TRUE	Subject Type=CA Path Length Constraint=None

(3) 下屬憑證機構憑證

擴充欄位	關鍵性	內容
憑證機構金鑰識別碼 (Authority Key Identifier)	FALSE	簽發者(Issuer)的公開金鑰 SHA-1 雜湊值
主體金鑰識別碼 (Subject Key Identifier)	FALSE	主體(Subject)的公開金鑰 SHA-1 雜湊值
CRL 發布點 (CRL Distribution Points)	FALSE	HiPKI RCA 公告之憑證機構廢止清冊的網址
憑證機構資訊存取 (Authority Information Access)	FALSE	此擴充欄位包含以下兩項資訊： ■ HiPKI RCA 之自簽憑證下載網址 ■ HiPKI RCA 所提供之線上憑證狀態協定查詢服務的網址
憑證政策 (Certificate Policies)	FALSE	此擴充欄位用於標示下屬憑證機構經 HiPKI RCA 核准並允許使用之憑證政策，可包含下述 1 個或多個憑證政策物件識別碼，並可視憑證需求使用政策限定元，用於標示本作業基準公告之網址。可使用之憑證政策物件識別碼包含： ■ 本基礎建設憑證政策定義之憑證政策物件識別碼 ■ 本基礎建設憑證政策引用之 CA/Browser Forum 定義之憑證政策物件識別碼。
延伸金鑰用途 (Extended Key Usage)	FALSE	此擴充欄位應包含下屬憑證機構欲使用之延伸金鑰用途資訊，但其延伸金鑰用途不可同時包含 id-kp-serverAuth 與 id-kp-emailProtection。
金鑰用途 (Key Usage)	TRUE	此擴充欄位內容可為下述其中一種： ■ keyCertSign 與 cRLSign (預設) ■ digitalSignature、keyCertSign 及 cRLSign (若下屬憑證機構欲使用其簽章用私密金鑰簽發線上憑證狀態協定回應訊息時，則此擴充欄位須包含 digitalSignature、keyCertSign 及 cRLSign。)
基本限制 (Basic Constraints)	TRUE	Subject Type=CA Path Length Constraint=依下屬憑證機構所需之憑證路徑長度限制設定之。

(4) 交互憑證

擴充欄位	關鍵性	內容
憑證機構金鑰識別碼 (Authority Key Identifier)	FALSE	簽發者(Issuer)的公開金鑰 SHA-1 雜湊值
主體金鑰識別碼 (Subject Key Identifier)	FALSE	主體(Subject)的公開金鑰 SHA-1 雜湊值
CRL 發布點 (CRL Distribution Points)	FALSE	HiPKI RCA 公告之憑證機構廢止清冊的網址
憑證機構資訊存取 (Authority Information Access)	FALSE	此擴充欄位包含以下兩項資訊： ■ HiPKI RCA 之自簽憑證下載網址 ■ HiPKI RCA 所提供之線上憑證狀態協定查詢服務的網址
憑證政策 (Certificate Policies)	FALSE	此擴充欄位用於標示交互認證憑證機構經 HiPKI RCA 核准並允許使用之憑證政策，可包含下述 1 個或多個憑證政策物件識別碼，並可視憑證需求使用政策限定元，用於標示本作業基準公告之網址。可使用之憑證政策物件識別碼包含： ■ 本基礎建設憑證政策定義之憑證政策物件識別碼 ■ 本基礎建設憑證政策引用之 CA/Browser Forum 定義之憑證政策物件識別碼。
憑證政策對應 (Policy Mappings)	FALSE	此擴充欄位用於標示交互認證憑證機構與總管理中心之憑證政策的對等關係，可有 1 個或多個憑證政策對。每個憑證政策對顯示 HiPKI RCA 之憑證政策物件識別碼與交互認證憑證機構所遵循之憑證政策物件識別碼相同。
金鑰用途 (Key Usage)	TRUE	此擴充欄位內容可為下述其中一種： ■ keyCertSign 與 cRLSign (預設) ■ digitalSignature、keyCertSign 及 cRLSign (若交互憑證機構欲使用其簽章用私密金鑰簽發線上憑證狀態協定回應訊息時，則此擴充欄位須包含 digitalSignature、keyCertSign 及 cRLSign。)
基本限制 (Basic Constraints)	TRUE	Subject Type=CA Path Length Constraint=依交互認證憑證機構所需之憑證路徑長度限制設定之。

此外，HiPKI RCA 不允許簽發下述兩種情境之憑證：

(1) 憑證的擴充欄位內含無法應用於公眾網路(Public Internet)的設定，例如：延伸金鑰用途擴充欄位包含僅適用於私有網路服務的設定值。

(2) 憑證的內容包含可能誤導信賴憑證者相信該憑證資訊已經由 HiPKI RCA 驗證之語意。

HiPKI RCA 不提供用戶憑證的簽發作業；換言之，亦不執行 RFC 6962 所定義之預簽憑證的簽發。

7.1.3 演算法物件識別碼

HiPKI RCA 簽發的憑證於簽章時可使用下述任一種演算法之物件識別碼：

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

(OID：1.2.840.113549.1.1.11)

sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}

(OID：1.2.840.113549.1.1.12)

sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}

(OID：1.2.840.113549.1.1.13)

ecdsaWithSHA256	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}

(OID：1.2.840.10045.4.3.2)

ecdsaWithSHA384	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)}

(OID：1.2.840.10045.4.3.3)

ecdsaWithSHA512	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)}

(OID：1.2.840.10045.4.3.4)

HiPKI RCA 簽發的憑證必須使用下述之物件識別碼來識別產製主體金鑰的演算法：

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}

(OID：1.2.840.113549.1.1.1)

ecPublicKey	{iso(1) member-body(2) us(840) ansi-x962(10045) keyType(2) ecPublicKey(1)}

(OID：1.2.840.10045.2.1)

若 HiPKI RCA 簽發的憑證使用 ECC 演算法產製主體金鑰時，將依其主體金鑰長度註記對應之橢圓曲線參數物件識別碼，可使用之物件識別碼包括：

secp256r1	{iso(1) member-body(2) us(840) ansi-x962(10045) curves(3) prime(1) prime256v1(7)}

(OID：1.2.840.10045.3.1.7)

secp384r1	{iso(1) identified-organization(3) certicom(132) curve(0) ansip384r1(34)}

(OID：1.3.132.0.34)

7.1.4 命名形式

憑證之主體及簽發者兩個欄位值使用 X.500 唯一識別名稱，此名稱的屬性型態遵循 ITU-T X.509、Baseline Requirements 及 RFC 5280 之規定。

HiPKI RCA 所簽發之自簽憑證、自發憑證、下屬憑證機構憑證以及交互憑證之簽發者欄位內容須與其自簽憑證的主體欄位內容相同。

HiPKI RCA 的自簽憑證，其主體唯一識別名稱包含 3 個屬性，分別為一般名稱(commonName)、組織名稱(organizationName)及國家代碼(countryName)，說明如下：

(1) 一般名稱

用於記載可識別HiPKI RCA之名稱，此名稱為此憑證的唯一識別碼，可作為與其他憑證區分之用。

(2) 組織名稱

用於記載HiPKI RCA所屬的正式組織名稱，其組織身分鑑別依第3.2.2節之規定進行。

組織名稱可與身分鑑別時所驗證的名稱有些微差異，以縮寫文字為例，組織名稱的部分文字可使用我國認可之縮寫方式進行調整，例如「Chunghwa Telecom Company Limited」改為「Chunghwa Telecom Co., Ltd.」。

(3) 國家代碼

用於記載HiPKI RCA營業地點(Place of Business)所在之國家，以符合ISO 3166-1國際標準所規範的國家代碼表示之。

HiPKI RCA 藉由簽發自發憑證、下屬憑證機構憑證及交互憑證，表示 HiPKI RCA 在憑證的簽發日期前已遵循憑證政策與/或本作業基準所闡述的程序來作驗證，確保所有記載於憑證之主體資訊的值是準確的。

7.1.5 命名限制

HiPKI RCA 不採用命名限制。對於不受技術約束(Technically Constrained)的自簽憑證、自發憑證、下屬憑證機構憑證及交互憑證，將透過 Mozilla 之 CCADB 與其他公開管道予以揭露。

7.1.6 憑證政策物件識別碼

HiPKI RCA 的自簽憑證不含憑證政策擴充欄位。

HiPKI RCA 簽發的自發憑證、下屬憑證機構憑證或交互憑證，其憑證政策擴充欄位除可使用本基礎建設憑證政策定義之憑證政策物件識別碼，亦可包含本基礎建設憑證政策引用之 CA/Browser Forum 定義之憑證政策物件識別碼，有關於憑證政策物件識別碼之相關說明請參閱第 1.2 節。

7.1.7 政策限制擴充欄位之使用

HiPKI RCA 簽發之下屬憑證機構與交互憑證，必要時將使用政策限制擴充欄位。

7.1.8 政策限定元之語法及語意

HiPKI RCA 簽發之自發憑證、下屬憑證機構憑證及交互憑證可視該憑證需求於憑證政策擴充欄位中使用政策限定元，用於標示本作業基準公告之網址。

7.1.9 關鍵憑證政策擴充欄位之語意處理

HiPKI RCA 簽發之憑證所含之憑證政策擴充欄位不註記為關鍵擴充欄位。

7.2 憑證廢止清冊之格式剖繪

7.2.1 版本序號

HiPKI RCA 簽發遵循 RFC 5280 與 ITU-T X.509 v2 版本的憑證機構廢止清冊。

7.2.2 憑證機構廢止清冊及憑證機構廢止清冊條目之擴充欄位

HiPKI RCA 簽發的憑證機構廢止清冊，其憑證廢止清冊擴充欄位(crlExtensions)及憑證廢止清冊條目擴充欄位(crlEntryExtensions)依照 ITU-T X.509、Baseline Requirements 及 RFC 5280 之規定。

7.3 線上憑證狀態協定之格式剖繪

HiPKI RCA 提供符合 RFC 6960 及 RFC 5019 標準規範之線上憑證狀態協定查詢服務，並在自發憑證、下屬憑證機構憑證及交互憑證的憑證機構資訊存取擴充欄位中包含 HiPKI RCA 線上憑證狀態協定查詢服務的服務網址。

7.3.1 版本序號

HiPKI RCA 的線上憑證狀態協定查詢封包應包含以下資訊：

- 版本序號
- 待查憑證識別碼(Identifier)

待查憑證識別碼包含：雜湊函數演算法、憑證簽發者名稱之雜湊值、憑證簽發者公開金鑰之雜湊值及待查詢憑證之憑證序號。

HiPKI RCA 簽發的線上憑證狀態協定回應封含有以下基本欄位：

欄位	說明
版本序號(Version)	v.1 (0x0)
線上憑證狀態協定回應伺服器 ID(Responder ID)	線上憑證狀態協定回應伺服器的主體名稱(Subject DN)
產製時間(Produced Time)	回應封包簽署時間
待查詢憑證識別碼(identifier)	包含：雜湊函數演算法、憑證簽發者名稱之雜湊值、憑證簽發者公開金鑰

欄位	說明
	之雜湊值及待查詢憑證之憑證序號
憑證狀態碼(Certificate Status)	憑證狀態對應碼(0:有效/1:廢止/2:未知)
效期 (ThisUpdate/NextUpdate)	此回應封包建議的效期區間，包含：生效時間(ThisUpdate)及下次更新時間(NextUpdate)
簽章演算法(Signature Algorithm)	回應封包的簽章演算法，為 sha256WithRSAEncryption
簽體(Signature)	線上憑證狀態協定回應伺服器的簽章
憑證(Certificates)	線上憑證狀態協定回應伺服器的憑證

7.3.2 線上憑證狀態協定擴充欄位

HiPKI RCA 線上憑證狀態協定的回應封包含有以下擴充欄位：

- 線上憑證狀態協定回應伺服器的憑證機構金鑰識別碼。
- 此外當線上憑證狀態協定查詢封包含有隨機數(Nonce)欄位時，線上憑證狀態協定回應封包也必須包含相同的隨機數欄位。

8 稽核及其他評核

8.1 稽核頻率或評核事項

HiPKI RCA 接受每年 1 次的外部稽核(且查核期間不可超過 12 個月)與不定期的內部稽核，以確認相關運作確實遵循 HiPKI 憑證政策及本作業基準所訂的安全規定與程序。稽核採用的標準為 WebTrust for CA、WebTrust for CA－SSL BR 及 WebTrust for CA－EV SSL。

8.2 稽核人員之身分及資格

本公司將委外辦理 HiPKI RCA 之外部稽核作業，委託熟悉 HiPKI RCA、下屬憑證機構運作並經 WebTrust for CA 標章管理單位授權可於中華民國執行 WebTrust for CA、 WebTrust for CA – EV SSL 及 WebTrust for CA – SSL BR 稽核標準之合格稽核業者，提供公正客觀的稽核服務。稽核人員應為合格授權之資訊系統稽核員(Certified Information System Auditor)或具同等資格，且具備 2 場次 4 人天以上之憑證機構 WebTrust for CA 標章稽核或 2 場次共計 8 人天憑證機構資訊安全管理稽核相關經驗，HiPKI RCA 於稽核時應對稽核人員進行身分識別。

8.3 稽核人員及被稽核方之關係

本公司將委託公正之第三方，就 HiPKI RCA 的運作進行稽核。

8.4 稽核項目

稽核項目如下所述：

(1) HiPKI RCA 是否遵照本作業基準運作

(2) 本作業基準是否符合憑證政策之規定

(3) 憑證機構與其他根憑證機構簽訂交互認證協議書(Cross Certification Agreement, CCA)時，稽核之項目應涵蓋該根憑證機構是否符合交互認證協議書之規定

8.5 對於稽核結果之因應方式

如稽核人員發現 HiPKI RCA 之建置與維運不符合本作業基準規定時，採取以下行動：

(1) 記錄不符合情形

(2) 將不符合情形通知 HiPKI RCA，如不符合情形為嚴重缺失，稽核人員應通知政策管理委員會

對於不符合規定之項目，HiPKI RCA 將於 30 日內提出改善計畫，儘速執行，並列入後續稽核追蹤項目。

8.6 稽核結果之公開

除可能導致系統被攻擊以及第 9.3 節規定之範圍外，HiPKI RCA 將公布合格稽核業者所提供之應公開說明資訊。稽核結果以 WebTrust for CA、WebTrust for CA－EV SSL 或 WebTrust for CA－SSL BR 標章之方式呈現於 HiPKI RCA 網站首頁，點選標章後可閱覽外稽報告與管理聲明書。最近 1 次的外稽報告與管理聲明書亦於查核區間結束後 3 個月內公布於儲存庫。若因故延遲公布最近 1 次稽核結果，HiPKI RCA 將提供合格稽核業者簽署之解釋函。

9 其他業務及法律事項

9.1 費用

HiPKI RCA 保留向下屬憑證機構、申請交互憑證之憑證機構收取費用的權利，該項費用限應用於 HiPKI RCA 的營運費用。

HiPKI RCA 如向下屬憑證機構、申請交互憑證之憑證機構收取費用，將配合修正本作業基準，並訂定相關費用之查詢方法及請求退費之程序。

9.1.1 憑證簽發、展期費用

目前沒有收費。

9.1.2 憑證查詢費用

目前沒有收費。

9.1.3 憑證廢止、狀態查詢費用

目前沒有收費。

9.1.4 其他服務費用

目前沒有收費。

9.1.5 退費

目前沒有收費，因此無請求退費之程序。

9.2 財務責任

9.2.1 保險涵蓋範圍

HiPKI RCA 由本公司營運，其財務責任由本公司負責。HiPKI RCA 憑證業務目前尚未辦理保險，未來將遵守主管機關規定加入保

險。

9.2.2 其他資產

HiPKI RCA 之財務，係屬本公司整體財務之一部。本公司為股票上市公司，依證券交易法第 36 條之規定，應於每營業年度終了後 3 個月內公告，並向主管機關申報，經會計師查核簽證，董事會通過及監察人承認之年度財務報告。並於每會計年度第 1 季、第 2 季及第 3 季終了後 45 日內，公告並申報經會計師核閱及提報董事會之財務報告。於每月 10 日以前，公告並申報上月份營運情形。HiPKI RCA 可提供自我擔保之資產價值依本公司年度財務報告為準。本公司財務健全，流動資產與流動負債比符合 EV SSL Certificate Guidelines 要求不低於 1.0 的要求。

9.2.3 對終端個體之保險或保固

不做規定。

9.3 業務資訊之保密

9.3.1 機密資訊之範圍

由 HiPKI RCA 產生、接收或保管之資料，均視為機密資訊，現職及曾任職於 HiPKI RCA 之人員與各類稽核人員對於機密資訊均負保密責任。機密資訊包括：

(1) 用於 HiPKI RCA 營運的私密金鑰及通行碼
(2) HiPKI RCA 金鑰分持的保管資料
(3) 下屬憑證機構之申請資料，未經下屬憑證機構同意或符合法令規定不得公開
(4) 交互認證憑證機構之申請資料，未經交互認證憑證機構同意或符合法令規定不得公開

(5) HiPKI RCA 產生或保管之可供稽核及追蹤之紀錄

(6) 稽核人員於稽核過程中產生之稽核紀錄及報告，不得被完整公開

(7) 列為機密等級的營運相關文件

9.3.2 非機密之資訊

(1) 識別資訊或記載於憑證的資訊，除特別約定外，不視為機密資訊。

(2) HiPKI RCA 儲存庫公布之簽發憑證、已廢止憑證及憑證機構廢止清冊不視為機密資訊

9.3.3 保護機密資訊之責任

HiPKI RCA 依照電子簽章法、Baseline Requirements、EV SSL Certificate Guidelines、WebTrust for CA 標準、WebTrust for CA－EV SSL 標準、WebTrust for CA－SSL BR 標準及個人資料保護法處理 HiPKI RCA 之下屬憑證機構及交互認證憑證機構的申請資料。

HiPKI RCA 實施安控措施防止機密資訊遭揭露或洩漏。

9.4 個人資訊之隱私

9.4.1 隱私保護計畫

HiPKI RCA 於網站公告個人資料保護與隱私權聲明。HiPKI RCA 實施隱私衝擊分析、個資風險評鑑等措施以訂定隱私保護計畫。

9.4.2 視為隱私之資訊

(1) 任何在憑證申請時記載之個人資訊皆為隱私資訊，未經申請者或授權代表人同意或依法令規定不得公開

(2) 憑證機構信賴角色維運之可識別的個人資料如姓名搭配掌紋特徵與指紋特徵

(3) 保密協定或契約之個人資訊

HiPKI RCA 實施安控措施防止隱私資料遭未經授權的揭露或洩漏。

9.4.3 非隱私之資訊

識別資訊、記載於憑證的資訊及憑證，除特別約定外，不應視為隱私資訊。

9.4.4 保護隱私資訊之責任

配合 HiPKI RCA 運作所需之個人資料，無論紙本或是電子之形式，必須依照於網站公告的個人資料保護暨隱私權聲明，安全存放與受到保護，符合電子簽章法、WebTrust for CA 標準及個人資料保護法相關規定。

9.4.5 使用隱私資訊之告知及同意

遵循個人資料保護法，非經當事人同意或 HiPKI RCA 網站公告之個人資料保護與隱私權聲明與本作業基準另有規範，不會將個人資料用於其他地方。

9.4.6 應司法或管理程序釋出資訊

司法機關、監察機關或治安機關如因調查或蒐集證據需要，必須查詢 9.4.2 節隱私資訊，依法令規定辦理；惟 HiPKI RCA 保留向申請查詢之機關收取合理費用之權利。

9.4.7 其他資訊釋出之情況

下屬憑證機構得查詢第 9.3.1 節第(3)款之申請資料；惟 HiPKI RCA 保留向申請查詢之下屬憑證機構收取合理費用之權利。

交互認證憑證機構得查詢第 9.3.1 節第(4)款之申請資料；惟 HiPKI

RCA 保留向申請查詢之交互認證憑證機構收取合理費用之權利。

其他資訊釋出之情況依相關規定法令辦理。

9.5 智慧財產權

HiPKI RCA 的金鑰對及金鑰分持之所有權為 HiPKI RCA 所擁有。下屬憑證機構與交互認證憑證機構的金鑰對為該憑證機構所有，但其公開金鑰經 HiPKI RCA 簽發成憑證時，該憑證之所有權亦為 HiPKI RCA 所擁有。

HiPKI RCA 簽發的憑證及憑證機構廢止清冊之所有權為 HiPKI RCA 所擁有。

HiPKI RCA 簽發的自簽憑證及自發憑證所記載之憑證主體名稱為 HiPKI RCA 所有。

HiPKI RCA 將儘可能確保下屬憑證機構與交互認證憑機構名稱的正確性，但不保證下屬憑證機構與交互認證憑證機構名稱之商標權歸屬。下屬憑證機構與交互認證憑證機構名稱如發生註冊商標爭議時，下屬憑證機構與交互認證憑證機構應依法定程序處理，並將處理結果提交 HiPKI RCA，以確保權益。

本作業基準可由儲存庫自由下載，或依著作權法相關規定重製或散布，但必須保證是完整複製，並註明著作權為本公司所擁有。重製或散布本作業基準者，不得向他人收取費用，對於不當使用或散布本作業基準之侵害，本公司將依法予以追訴。

9.6 聲明及擔保

9.6.1 HiPKI RCA 之聲明及擔保

HiPKI RCA 向憑證之受益人(包括下屬憑證機構、信賴憑證者及應用軟體供應商)聲明及擔保在憑證效期內，係遵照憑證政策及本作

業基準之規定進行憑證之簽發及管理。

具體地憑證擔保包含(但不限於)以下事項：

(1) 憑證授權

於憑證核發時，HiPKI RCA 會(i)驗證憑證之主體已授權憑證之簽發且申請代表人為憑證之主體所授權進行憑證請求；(ii)依照此程序進行憑證之簽發；及(iii)正確地將此程序描述於本作業基準(參見第 3.2.5 節)。

(2) 資訊正確性

於憑證核發時，HiPKI RCA 會(i)驗證記載於憑證內之所有資訊的正確性(除了憑證主體的附屬單位(organizationalUnitName)屬性以外)；(ii)依照此程序進行憑證之簽發；及(iii)正確地將此程序描述於本作業基準(參見第 3.2.2、第 3.2.3 及第 3.2.7 節)。

(3) 無誤導資訊

於憑證核發時，HiPKI RCA 會(i)降低記載於憑證主體附屬單位的資訊可能會造成誤導之可能性；(ii)依照此程序進行憑證之簽發；及(iii)正確地將此程序描述於本作業基準(參見第 3.2.2、第 3.2.3 及第 3.2.7 節)。

(4) 申請者的身分

若憑證中包含主體身分資訊，HiPKI RCA 會(i)依照第 3.2.2 及第 3.2.3 節的規定驗證申請者之身分；(ii)依照此程序進行憑證之簽發；及(iii)正確地將此程序描述於本作業基準。

(5) 用戶協議

若 HiPKI RCA 與下屬憑證機構非隸屬同一組織，則下屬

憑證機構與 HiPKI RCA 是符合 Baseline Requirements 要求之合法有效且可執行用戶協議的當事方；若 HiPKI RCA 與下屬憑證機構隸屬同一組織，則由申請代表人確認使用條款。

(6) 狀態

HiPKI RCA 維護一個 24 x 7 可公開存取的儲存庫，其中包含所有未到期憑證狀態(有效或已廢止)的最新資訊(參見第 4.10.2 節)。

(7) 廢止

HiPKI RCA 將根據 Baseline Requirements 及/或 EV SSL Certificate Guidelines 中所規定的任何理由廢止憑證(參見第 4.9.1 節)。

9.6.2 註冊中心之聲明及擔保

HiPKI RCA 不設置註冊中心。

9.6.3 下屬憑證機構及交互認證憑證機構之聲明及擔保

9.6.3.1 下屬憑證機構之聲明及擔保

下屬憑證機構聲明及擔保以下責任：

(1) 遵守本作業基準之規定，如未遵守導致信賴憑證者遭受損害時，應負損害賠償責任

(2) HiPKI RCA 簽發之憑證，依據憑證政策的規定，不同保證等級有不同之適用範圍，下屬憑證機構於提出憑證申請時，必須敘明所申請憑證之保證等級

(3) 下屬憑證機構申請憑證應依照第 4.2 節之程序進行申請，並確認申請資料之正確性

(4) 在核可下屬憑證機構之憑證申請及 HiPKI RCA 簽發憑證後，下屬憑證機構應依照第 4.4 節規定接受憑證

(5) 下屬憑證機構在接受 HiPKI RCA 所簽發之憑證後，即表示已確認憑證內容資訊之正確性，並依照第 1.4.1 節規定使用憑證

(6) 下屬憑證機構應依照第 6 章規定，自行產製私密金鑰

(7) 下屬憑證機構應妥善保管及使用私密金鑰

(8) 使用與憑證之公開金鑰相對應之私密金鑰簽署之數位簽章即為下屬憑證機構之數位簽章，下屬憑證機構在產生數位簽章時，必須確認已接受該下屬憑證機構憑證，且該憑證仍在有效期間並未被廢止

(9) 下屬憑證機構如發生第 4.9.1 節廢止憑證之事由(如私密金鑰外洩或遺失)，必須廢止憑證時，應立即通知 HiPKI RCA，如未通知或通知後尚未異動前，下屬憑證機構仍應承擔使用該憑證之法律責任

(10) HiPKI RCA 如因故無法正常運作時，下屬憑證機構應儘速尋求其他途徑完成與他人應為之法律行為，不得以 HiPKI RCA 無法正常運作，作為抗辯他人之事由

9.6.3.2 交互認證憑證機構之聲明及擔保

交互認證憑證機構聲明及擔保以下責任：

(1) 遵守本作業基準及交互認證協議之規定，如未遵守導致信賴憑證者遭受損害時，應負損害賠償責任

(2) HiPKI RCA 簽發之憑證，依據憑證政策的規定，不同保證等級有不同之適用範圍，交互認證憑證機構於提出交互認證申請時，必須敘明所申請憑證之保證等級

(3) 依照第 4.2 節之程序進行交互認證憑證申請，並確認申請資

料之正確性

(4) 在交互認證憑證申請核可及 HiPKI RCA 簽發憑證後，交互認證憑證機構應依照第 4.4 節規定接受憑證

(5) 交互認證憑證機構在接受 HiPKI RCA 所簽發之憑證後，即表示已確認憑證內容資訊之正確性，並依照第 1.4.1 節規定使用憑證。

(6) 申請交互認證之憑證機構應依照第 6 章規定，自行產製私密金鑰

(7) 交互認證憑證機構應妥善保管及使用私密金鑰

(8) 使用與憑證之公開金鑰相對應之私密金鑰簽署之數位簽章即為交互認證憑證機構之數位簽章，交互認證憑證機構在產生數位簽章時，必須確認已接受該憑證，且該憑證仍在有效期間並未被廢止

(9) 交互認證憑證機構如發生第 4.9.1 節廢止憑證之事由(如私密金鑰外洩或遺失)，必須廢止憑證時，應立即通知 HiPKI RCA，並依照第 4.9 節規定辦理憑證停用或廢止，如未通知或通知後尚未異動前，交互認證憑證機構仍應承擔使用該憑證之法律責任

(10)HiPKI RCA 如因故無法正常運作時，交互認證憑證機構應儘速尋求其他途徑完成與他人應為之法律行為，不得以 HiPKI RCA 無法正常運作，作為抗辯他人之事由

9.6.4 信賴憑證者之聲明及擔保

信賴憑證者應聲明與擔保以下之責任：

(1) 使用憑證或查詢 HiPKI RCA 儲存庫時，必須遵守本作業基準之相關規定

(2) 應依照第 6.1.4 節所述之自簽憑證安全散布管道取得所信賴的 HiPKI RCA 之公開金鑰或自簽憑證

(3) 使用憑證前，應先查驗該憑證之保證等級

(4) 使用憑證前，應先檢驗憑證之用途限制，以確認該憑證之使用確實符合 HiPKI RCA 設定之用途限制

(5) 使用 HiPKI RCA 簽發之憑證機構廢止清冊或線上憑證狀態協定查驗 HiPKI RCA 簽發之憑證，以確認該憑證之有效性

(6) 信賴憑證者在 HiPKI RCA 更換金鑰後使用其簽發之憑證時，應到 HiPKI RCA 的儲存庫取得自發憑證，以建構 HiPKI RCA 與憑證機構間之憑證信賴路徑

(7) 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信賴憑證者權益受損時，信賴憑證者應自行承擔責任

(8) HiPKI RCA 如因故無法正常運作時，信賴憑證者應儘速尋求其他途徑完成與他人應為之法律行為

(9) 接受 HiPKI RCA 簽發之憑證時，即視為已了解並同意有關本管理中心法律責任之條款，並依照第 1.4.1 節規定範圍使用憑證

9.6.5 其他參與者之聲明及擔保

不做規定。

9.7 免責聲明

除法令或本作業基準另有規範禁止之範圍外，HiPKI 在此特別對商品使用及特定目的合用性之明示及暗示的保證作免責聲明。

9.8 責任限制

下屬憑證機構、交互認證憑證機構或信賴憑證者如未依照 Baseline Requirements 及本作業基準之適用範圍使用憑證所引發之損失，HiPKI 不負任何賠償責任。若屬可歸咎於 HiPKI 之責任，其賠償金額上限依照本作業基準第 9.9 節規範。

9.9 賠償

9.9.1 HiPKI RCA 之賠償責任

(1) 如因 HiPKI RCA 作業人員故意或過失，未依憑證實務作業基準之規定，辦理自簽憑證、自發憑證、下屬憑證機構憑證與交互憑證之簽發與廢止作業，或違反相關法律規範而造成 HiPKI RCA、下屬憑證機構或交互認證憑證機構或信賴憑證者之損失時，HiPKI RCA 應依規定賠償其直接損失。

(2) 如因第 9.16.5 節不可抗力之因素，導致 HiPKI RCA 所簽發之憑證造成損失時，HiPKI RCA 不負任何損害賠償責任。

(3) 憑證機構或其他有權者提出廢止憑證之要求後，至 HiPKI RCA 實際完成廢止該憑證機構憑證為止之期間內，當該憑證機構憑證被用以進行非法交易，或進行交易後產生法律糾紛時，HiPKI RCA 如依據本作業基準與相關之作業規範執行處理作業時，則不負任何損害賠償責任。

(4) 下屬憑證機構、交互認證憑證機構或信賴憑證者如未依照第 1.4.1 節規定之適用範圍使用憑證所引發之損失，HiPKI RCA 不負任何損害賠償責任

(5) 賠償追究有效期限，依電子簽章法主管機關與相關法令之規範辦理。

9.9.2 下屬憑證機構及交互認證機構之賠償責任

HiPKI RCA 在法律規範下，得要求下屬憑證機構與交互認證機構於下述情形造成直接損害時，應負擔賠償責任：

(1) 下屬憑證機構或交互認證機構於憑證申請時提供虛假或欺詐的陳述，造成 HiPKI RCA 簽發了不正確的憑證機構憑證或交互認證憑證。

(2) 下屬憑證機構或交互認證機構未妥善保管其私密金鑰，導致私密金鑰遭破解、揭露、修改或未經授權的使用。

(3) 下屬憑證機構或交互認證機構違反法律、憑證政策或本作業基準(如未依照憑證實務作業基準規定之保證等級簽發適當之憑證)、交互認證協議之規定，。

(4) 下屬憑證機構或交互認證機構違背 HiPKI RCA 參與各作業系統、瀏覽器與軟體平台之根憑證計畫所簽署之協議，甚至影響了 HiPKI RCA 在上述應用軟體供應商已經植入或即將申請植入之憑證機構信賴清單。

HiPKI RCA 得於交互認證協議約定下屬憑證機構或交互認證機構賠償之責任。

9.10 有效期限及終止

9.10.1 有效期限

本作業基準和修訂之版本於電子簽章法主管機關核定並公告於 HiPKI RCA 網站與儲存庫時生效，且直到被新的版本取代前仍然有效。

9.10.2 終止

本作業基準和修訂之版本直到被電子簽章法主管機關核定之新

的版本取代前仍然有效。

9.10.3 效力之終止及保留

透過 HiPKI RCA 網站與儲存庫溝通本作業基準效力終止的狀況和影響。此溝通將強調本作業基準效力終止的保留情形，最起碼保護機密資訊的相關責任在本作業基準終止後仍將保留。

9.11 主要成員之個別告知及溝通

HiPKI RCA、下屬憑證機構、交互認證憑證機構及信賴憑證者彼此間得採適當的方式，建立通告與聯絡管道，包括但不限於：公文、書信、電話、傳真、電子郵件或安全電子郵件。

9.12 修訂

9.12.1 修訂程序

本作業基準每年定期審視並評估是否需要修訂，以維持其保證度。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，且以適當之版本編號代表本作業基準有進行修訂。

9.12.2 通知之機制及期限

重大變更項目及修訂之憑證實務作業基準生效日期將公告於 HiPKI RCA 網站，並透過發函或電子郵件通知非本公司設立之下屬憑證機構與交互認證憑證機構有關修訂的內容。憑證機構或信賴憑證者對於變更項目有意見者，可於公告之意見回覆期限截止前提出，由 HiPKI RCA 考量相關意見，評估變更項目與回覆。

本作業基準重新排版時，不另作通知。

9.12.3 物件識別碼必須更改之情況

憑證政策的修改不影響憑證政策所聲明的憑證使用目的與保證度時，憑證政策之物件識別碼不需修改，憑證政策之物件識別碼變更，憑證實務作業基準應作相對應之變更。

9.13 爭議解決條款

本公司所屬憑證機構與 HiPKI RCA 如有爭議時，依本公司組織管理體制，由共同上級主管調處解決。非本公司設立之交互認證憑證機構與 HiPKI RCA 如有爭議時，應先進行協商以取得共識。如協商不成時，依雙方契約約定之紛爭處理程序處理。如需訴訟時，以臺灣臺北地方法院為第一審管轄法院。

9.14 管轄法律

牽涉 HiPKI RCA 所簽發之憑證的任何爭議由中華民國相關法令規定管轄。

9.15 適用法律

依據憑證政策及本作業基準所簽署的任何協議之解釋及合法性，必須遵循中華民國相關法令規定。

9.16 雜項條款

9.16.1 完整協議

本作業基準所約定者，構成主要成員間最終且完整的約定。主要成員間就同一事項縱使先前曾以口頭或書面有其他的表示，最終仍應以本作業基準之約定為準。

9.16.2 轉讓

本作業基準所敘述的主要成員(HiPKI RCA、下屬憑證機構、交互認證憑證機構、信賴憑證者)之間的權利或責任，不能在未通知HiPKI RCA 下以任何形式轉讓給其他方。

9.16.3 可分割性

如本作業基準的任一條款不正確或無效時，其他條款仍然有效，直到本作業基準修改為止。

本作業基準遵循 Baseline Requirements 及 EV SSL Certificate Guidelines 對根憑證機構之要求，惟 Baseline Requirements 及 EV SSL Certificates Guidelines 相關規定與本作業基準所依循之本國相關法律或法規產生衝突時，本作業基準得調整相關作法以滿足法律或法規之要求，並將變更調整之部分通知憑證機構與瀏覽器論壇；若本國法律或法規已不再適用時，或憑證機構與瀏覽器論壇修訂 Baseline Requirements 及 EV SSL Certificates Guidelines 之相關內容使其規定可相容於本國法律時，則本作業基準將刪除並修訂原先所調整之內容，上述作業須於 90 個工作天內完成。

9.16.4 契約履行

因可歸責於憑證機構或信賴憑證者之故意或過失違反本憑證作業基準相關規定，致 HiPKI RCA 受有損害時，HiPKI RCA 除得請求損害賠償以外，並得向可歸責之一方請求支付為處理該爭議或訴訟之律師費用。

HiPKI RCA 未向違反本憑證作業基準相關規定者主張權利，不代表 HiPKI RCA 對於其繼續或未來違反本憑證作業基準情事，有拋棄權利主張之意思。

9.16.5 不可抗力

因不可抗力或其他非可歸責於 HiPKI RCA 之事由致憑證機構或信賴憑證者受有損害，包含但不限於天災、戰爭、恐怖攻擊、或電信網路中斷等事件，HiPKI RCA 不負任何法律責任。

9.17 其他條款

不做規定。