# CA/Browser Forum 《Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates》 非官方繁體中文翻譯 — 全文（含附錄）

對應原文版本 2.3.0 • 匯出日期 2026-09-27 • 本檔僅含中文翻譯，未附英文原文。
內容範圍：全文（含附錄）（已完成人工審閱之章節）。

⚠ 本站為 Web PKI 相關文件的非官方繁體中文翻譯，由社群維護。發生爭議時以原文內容為準。本網站內容不構成法律意見。
本檔為參考用途，非 CA/Browser Forum 官方文件；原文請見 cabforum.org。

---

**目錄**

# 1 簡介

## 1.1 概要

本文件描述了一套整合技術、協定、身分查核（identity-proofing）、生命週期管理（lifecycle management）以及稽核要求（auditing requirements）之規範，這些要素皆為簽發（issuance）與管理公開信賴 TLS 伺服器憑證（Publicly-Trusted TLS Server Certificates）所必要（但非充分）之條件；憑證（Certificates）之所以受到信賴，是由於其對應之根憑證（Root Certificate）已內建於廣泛使用的應用軟體（application software）中。除非作為信賴憑證者（Relying Party）的應用軟體供應商（Application Software Suppliers）採納並強制執行本文件要求規定，否則這些要求對於憑證機構（Certification Authority，CA）並不具強制性。

### 讀者須知（Notice to Readers）

公開信賴 TLS 伺服器憑證簽發與管理之憑證政策（Certificate Policy，CP）描述憑證機構（Certification Authority，CA）簽發公開信賴 TLS 伺服器憑證所應符合之要求的一部分內容。本文件具有兩個目的：明定《基本要求》（Baseline Requirements）內容以及針對 CA 在其憑證實務作業基準（Certification Practice Statement，CPS）中宜包含的內容提供指引與要求。除非另有明確說明，否則本文件要求規定僅適用於 2012-07-01（本文件的原始生效日（effective date））或之後發生的相關事件。

本文件並未涵蓋簽發與管理公開信賴 TLS 伺服器憑證過程中所涉及的全部議題。為了依循 RFC 3647 規範，且利於與其他憑證政策（CP）及憑證實務作業基準（CPS）進行比對（例如用於政策對應（policy mapping)），本文件包含 RFC 3647 架構之所有章節。然而，CA/Browser Forum 並非在所有空白章節中皆以「不作規定」（no stipulation）註解開頭，而是將此類章節先保持空白，直到做出「不作規定」的決定為止。CA/Browser Forum 得不定期更新本文件要求規定，以因應現有及新興的網路安全（online security）威脅。具體而言，預計未來版本將針對受委託作業（delegated functions）包含更正式且全面的稽核要求（audit requirements）。

本文件要求規定僅針對用於鑑別（authenticating）可透過網際網路（Internet）存取之伺服器的憑證。針對程式碼簽章（code signing）、S/MIME、時戳（time-stamping）、VoIP、IM、Web 服務（Web services）等類似要求，可能會在未來版本中涵蓋。

本文件要求規定不涉及企業（enterprises）僅供內部用途（internal purposes）而自行營運的公開金鑰基礎建設（Public Key Infrastructure，PKI），及其所進行的憑證簽發或管理，且其根憑證（Root Certificate）未經任何應用軟體供應商（Application Software Supplier）配發。

本文件要求規定適用憑證信賴鏈（chain of trust）中的所有憑證機構（Certification Authorities）。這些要求應從根憑證機構（Root Certification Authority）向下傳遞至各級的下屬憑證機構（Subordinate Certification Authorities）。

## 1.2 文件名稱與識別

本憑證政策（Certificate Policy，CP）包含經 CA/Browser Forum 採納的公開信賴 TLS 伺服器憑證簽發與管理的相關要求。

下列憑證政策識別碼（Certificate Policy identifiers）保留供憑證機構（CA）使用，用以宣告憑證遵循本文件（OID arc 2.23.140.1.2）之規定，具體如下：

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1);` 以及

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2);` 以及

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) individual-validated(3)} (2.23.140.1.2.3)`。

### 1.2.1 版本修訂

| 版本 | Ballot 投票案 | 內容 | 採納日期 | 生效日* |
|---|---|---|---|---|
| 1.0.0 | 62 | 採納《基本要求》1.0 版 | 2011-11-22 | 2012-07-01 |
| 1.0.1 | 71 | 修訂稽核者（Auditor）資格 | 2012-05-08 | 2013-01-01 |
| 1.0.2 | 75 | 允許將非關鍵（Non-critical）Name Constraints 視為 RFC 5280 之例外 | 2012-06-08 | 2012-06-08 |
| 1.0.3 | 78 | 修訂網域／IP 位址驗證、高風險申請與資料來源 | 2012-06-22 | 2012-06-22 |
| 1.0.4 | 80 | 未簽發憑證之 OCSP 回應 | 2012-08-02 | 2013-08-02 |
| — | 83 | 採納《網路與憑證系統安全要求》（NCSSR） | 2013-08-03 | 2013-01-01 |
| 1.0.5 | 88 | 允許使用者指定國碼 XX | 2012-09-12 | 2012-09-12 |
| 1.1.0 | — | 以 1.1 版發布，內容與 1.0.5 相同 | 2012-09-14 | 2012-09-14 |
| 1.1.1 | 93 | 廢止事由與公開金鑰參數檢查 | 2012-11-07 | 2012-11-07 |
| 1.1.2 | 96 | 萬用字元（Wildcard）憑證與新通用頂級網域（New gTLD） | 2013-02-20 | 2013-02-20 |
| 1.1.3 | 97 | 防止未知的憑證內容 | 2013-02-21 | 2013-02-21 |
| 1.1.4 | 99 | 新增 DSA 金鑰（BR v.1.1.4） | 2013-05-03 | 2013-05-03 |
| 1.1.5 | 102 | 修訂第 9.2.3 節的主體網域元件（domainComponent）與語言（language）屬性 | 2013-05-31 | 2013-05-31 |
| 1.1.6 | 105 | 下屬憑證機構（Subordinate CA）的技術性約束 | 2013-07-29 | 2013-07-29 |
| 1.1.7 | 112 | 將「Internal Server Name」定義替換為「Internal Name」 | 2014-04-03 | 2014-04-03 |
| 1.1.8 | 120 | 關係企業（Affiliate）的網域驗證授權 | 2014-06-05 | 2014-06-05 |
| 1.1.9 | 129 | 第 11.1.3 節所述 PSL 之釐清 | 2014-08-04 | 2014-08-04 |
| 1.2.0 | 125 | CAA 紀錄 | 2014-10-14 | 2015-04-15 |
| 1.2.1 | 118 | SHA-1 淘汰時程 | 2014-10-16 | 2014-11-16 |
| 1.2.2 | 134 | 預簽憑證（Pre-certificates）對 RFC 5280 規範之適用 | 2014-10-16 | 2014-10-16 |
| 1.2.3 | 135 | ETSI 稽核者資格 | 2014-10-16 | 2014-10-16 |
| 1.2.4 | 144 | .onion 網域名稱的驗證規範 | 2015-02-18 | 2015-02-18 |
| 1.2.5 | 148 | 修正 Issuer 欄位 | 2015-04-02 | 2015-04-02 |

| 版本 | Ballot 投票案 | 內容 | 採納日期 | 生效日* |
|---|---|---|---|---|
| 1.3.0 | 146 | 將《基本要求》轉換為 RFC 3647 架構 | 2015-04-16 | 2015-04-16 |
| 1.3.1 | 151 | 新增選用 OID 以表示驗證等級 | 2015-09-28 | 2015-09-28 |
| 1.3.2 | 156 | 增修《基本要求》第 1、2 節 | 2015-12-03 | 2016-12-03 |
| 1.3.3 | 160 | 增修《基本要求》第 4 節 | 2016-02-04 | 2016-02-04 |
| 1.3.4 | 162 | 例外條款的淘汰時程 | 2016-03-15 | 2016-03-15 |
| 1.3.5 | 168 | 《基本要求》校正（修訂版） | 2016-05-10 | 2016-05-10 |
| 1.3.6 | 171 | 更新 CABF 文件中之 ETSI 標準 | 2016-07-01 | 2016-07-01 |
| 1.3.7 | 164 | 憑證序號的亂度（資訊熵） | 2016-07-08 | 2016-09-30 |
| 1.3.8 | 169 | 修訂驗證要求 | 2016-08-05 | 2017-03-01 |
| 1.3.9 | 174 | 改革與當地法律衝突時之相關要求 | 2016-08-29 | 2016-11-27 |
| 1.4.0 | 173 | 移除因資訊錯誤而須停用公鑰之要求 | 2016-07-28 | 2016-09-11 |
| 1.4.1 | 175 | 於主體欄位增訂 givenName 與 surname 屬性 | 2016-09-07 | 2016-09-07 |
| 1.4.2 | 181 | 移除第 3.2.2.4 節所列之部分驗證方法 | 2017-01-07 | 2017-01-07 |
| 1.4.3 | 187 | 強制執行 CAA 檢查 | 2017-03-08 | 2017-09-08 |
| 1.4.4 | 193 | 憑證有效期為 825 日 | 2017-03-17 | 2018-03-01 |
| 1.4.5 | 189 | 增修《基本要求》第 6.1.7 節 | 2017-04-14 | 2017-05-14 |
| 1.4.6 | 195 | CAA 修補 | 2017-04-17 | 2017-05-18 |
| 1.4.7 | 196 | 定義「稽核期間」（Audit Period） | 2017-04-17 | 2017-05-18 |
| 1.4.8 | 199 | 要求根憑證與中繼憑證須含 commonName 欄位 | 2017-05-09 | 2017-06-08 |
| 1.4.9 | 204 | 禁止受委任第三方（DTP）執行網域／IP 所有權驗證 | 2017-07-11 | 2017-08-11 |
| 1.5.0 | 212 | 規範《基本要求》正式名稱 | 2017-09-01 | 2017-10-01 |
| 1.5.1 | 197 | Ballot 193 條文之生效日 | 2017-05-01 | 2017-06-02 |
| 1.5.2 | 190 | 新增驗證方法與若干小幅修正 | 2017-09-19 | 2017-10-19 |
| 1.5.3 | 214 | CAA 檢索 CNAME 規則之內容勘誤 | 2017-09-27 | 2017-10-27 |
| 1.5.4 | 215 | 修正 Ballot 190 文字誤植 | 2017-10-04 | 2017-11-05 |
| 1.5.5 | 217 | RFC 2527 淘汰時程 | 2017-12-21 | 2018-03-09 |

| 版本 | Ballot 投票案 | 內容 | 採納日期 | 生效日* |
|---|---|---|---|---|
| 1.5.6 | 218 | 移除驗證方法 #1 與 #5 | 2018-02-05 | 2018-03-09 |
| 1.5.7 | 220 | 小幅整理（2018 春） | 2018-03-30 | 2018-04-29 |
| 1.5.8 | 219 | 明定未含 “issue” ／ “issuewild” 屬性標籤之 CAA 紀錄集（Record Set）處理方式 | 2018-04-10 | 2018-05-10 |
| 1.5.9 | 223 | 更新《基本要求》第 8.4 節之 CA 稽核準則 | 2018-05-15 | 2018-06-14 |
| 1.6.0 | 224 | WhoIs 與 RDAP | 2018-05-22 | 2018-06-22 |
| 1.6.1 | SC006 | 憑證廢止時限之延長 | 2018-09-14 | 2018-10-14 |
| 1.6.2 | SC012 | 於 dNSName 內容值使用底線字元（Underscore）之淘汰時程 | 2018-11-09 | 2018-12-10 |
| 1.6.3 | SC013 | CAA Contact 屬性及相關電子郵件驗證方法 | 2018-12-25 | 2019-02-01 |
| 1.6.4 | SC014 | 更新電話驗證方法 | 2019-01-31 | 2019-03-16 |
| 1.6.4 | SC015 | 移除第 9 號驗證方法 | 2019-02-05 | 2019-03-16 |
| 1.6.4 | SC007 | 更新 IP 位址驗證方法 | 2019-02-08 | 2019-03-16 |
| 1.6.5 | SC016 | 其他 Subject 屬性 | 2019-03-15 | 2019-04-16 |
| 1.6.6 | SC019 | 透過 DNS CAA Phone Contact v2 之電話聯絡 | 2019-05-20 | 2019-09-09 |
| 1.6.7 | SC023 | 預簽憑證（Precertificates） | 2019-11-14 | 2019-12-19 |
| 1.6.7 | SC024 | 秋季整理 v2 | 2019-11-12 | 2019-12-19 |
| 1.6.8 | SC025 | 定義新 HTTP 網域驗證方法 v2 | 2020-01-31 | 2020-03-03 |
| 1.6.9 | SC027 | 第 3 版 Onion 憑證 | 2020-02-19 | 2020-03-27 |
| 1.7.0 | SC029 | 調整 Markdown 格式相容 Pandoc | 2020-03-20 | 2020-05-04 |
| 1.7.1 | SC030 | 揭露公司註冊／設立登記機構 | 2020-07-13 | 2020-08-20 |
| 1.7.1 | SC031 | 與瀏覽器安全政策同步（Browser Alignment） | 2020-07-16 | 2020-08-20 |
| 1.7.2 | SC033 | TLS 驗證使用 ALPN 方法 | 2020-08-14 | 2020-09-22 |
| 1.7.3 | SC028 | 記錄與紀錄保留 | 2020-09-10 | 2020-10-19 |
| 1.7.3 | SC035 | 整理與釐清 | 2020-09-09 | 2020-10-19 |
| 1.7.4 | SC041 | 重新編排《基本要求（BRs）》、《EV 指引（EVGs）》與《網路與憑證系統安全要求（NCSSR）》 | 2021-02-24 | 2021-04-05 |

| 版本 | Ballot 投票案 | 內容 | 採納日期 | 生效日* |
|---|---|---|---|---|
| 1.7.5 | SC042 | 可重複使用（Re-use）已驗證資料之期限降為 398 日 | 2021-04-22 | 2021-06-02 |
| 1.7.6 | SC044 | 明定可接受的狀態碼 | 2021-04-30 | 2021-06-03 |
| 1.7.7 | SC046 | DNS 業者的 CAA 例外條款之淘汰時程 | 2021-06-02 | 2021-07-12 |
| 1.7.8 | SC045 | 萬用字元網域驗證 | 2021-06-02 | 2021-07-13 |
| 1.7.9 | SC047 | subject:organizationalUnitName 淘汰時程 | 2021-06-30 | 2021-08-16 |
| 1.8.0 | SC048 | 網域名稱與 IP 位址的表示格式規範 | 2021-07-22 | 2021-08-25 |
| 1.8.1 | SC050 | 移除第 4.1.1 節之要求 | 2021-11-22 | 2021-12-23 |
| 1.8.2 | SC053 | SHA-1 OCSP 簽章之淘汰時程 | 2022-01-26 | 2022-03-04 |
| 1.8.3 | SC051 | 縮減並明定紀錄與紀錄歸檔保留之要求 | 2022-03-01 | 2022-04-15 |
| 1.8.4 | SC054 | Onion 整理 | 2022-03-24 | 2022-04-23 |
| 1.8.5 | SC056 | 2022 整理 | 2022-10-25 | 2022-11-30 |
| 1.8.6 | SC058 | 要求分片式（Sharded）CRL 須含 distributionPoint 欄位 | 2022-11-07 | 2022-12-11 |
| 1.8.7 | SC061 | 新 CRL 記錄必須有廢止原因代碼（Revocation Reason Code） | 2023-04-01 | 2023-07-15 |
| 2.0.0 | SC062 | 更新憑證剖繪（Certificate Profiles） | 2023-04-22 | 2023-09-15 |
| 2.0.1 | SC063 | OCSP 改為選用、強制 CRL，並鼓勵自動化 | 2023-08-17 | 2024-03-15 |
| 2.0.2 | SC066 | 2023 整理 | 2023-11-23 | 2024-01-08 |
| 2.0.3 | SC069 | 明定路由器與防火牆的記錄要求 | 2024-03-13 | 2024-04-15 |
| 2.0.4 | SC065 | 將《EV 指引（EVGs）》轉為 RFC 3647 格式 | 2024-03-15 | 2024-05-15 |
| 2.0.5 | SC073 | 金鑰遭破解與弱金鑰 | 2024-05-03 | 2024-07-01 |
| 2.0.6 | SC075 | 簽章前的 Linting 檢查（Pre-sign linting） | 2024-06-28 | 2024-08-06 |
| 2.0.7 | SC067 | 強制實施多視角簽發佐證（MPIC） | 2024-08-02 | 2024-09-06 |
| 2.0.8 | SC077 | 更新第 8.4 節與參考資料內容的 WebTrust 稽核名稱 | 2024-09-02 | 2024-10-02 |
| 2.0.9 | SC078 | Subject organizationName 欄位比照 EV 憑證及 S/MIME 顯示 DBA／商業名稱（Assumed Name） | 2024-10-02 | 2024-11-08 |
| 2.1.0 | SC076 | 明定並改善 OCSP 要求 | 2024-09-26 | 2024-11-14 |

| 版本 | Ballot 投票案 | 內容 | 採納日期 | 生效日* |
|---|---|---|---|---|
| 2.1.1 | SC079 | 允許交互認證之下屬憑證機構憑證（Cross-Certified Subordinate CA Certificate）包含一個以上之憑證政策 | 2024-09-30 | 2024-11-14 |
| 2.1.2 | SC080 | 強化 WHOIS 查詢並淘汰第 3.2.2.4.2 節、第 3.2.2.4.15 節驗證方法 | 2024-11-07 | 2024-12-16 |
| 2.1.3 | SC083 | 2024-2025 冬季整理 Ballot | 2025-01-23 | 2025-02-24 |
| 2.1.4 | SC084 | 標記 ACME Account ID 的 DNS 驗證方法 | 2025-01-28 | 2025-03-01 |
| 2.1.5 | SC081 | 導入縮短憑證有效期與可重複使用已驗證資料之期限的時程表 | 2025-04-11 | 2025-05-16 |
| 2.1.6 | SC085 | 查詢 CAA 與 DCV 時，要求驗證 DNSSEC（當其存在時） | 2025-06-19 | 2025-07-21 |
| 2.1.7 | SC089 | 大規模廢止（Mass Revocation）規劃 | 2025-07-23 | 2025-08-25 |
| 2.1.8 | SC092 | 淘汰預簽憑證簽章憑證機構（Precertificate Signing CA） | 2025-10-03 | 2025-11-04 |
| 2.1.9 | SC088 | 基於持久性紀錄值之 DNS TXT 紀錄的 DCV 方法 | 2025-10-09 | 2025-11-10 |
| 2.2.0 | SC086 | 終止 Address and Routing Parameter Area (.arpa) 網域名稱的憑證申請 | 2025-11-13 | 2025-12-15 |
| 2.2.1 | SC091 | 淘汰第 3.2.2.5.3 節反向位址查詢驗證， | 2025-11-13 | 2025-12-16 |
| 2.2.1 | SC091 | 新增使用持久性 DCV TXT 紀錄之 IP 位址 DNS 驗證方法 | 2025-11-13 | 2025-12-16 |
| 2.2.2 | SC090 | 逐步淘汰剩餘的電子郵件、電話驗證與「crossover」驗證方法 | 2025-11-20 | 2026-01-12 |
| 2.2.3 | SC094 | 電子郵件 DCV 方法之 DNSSEC 豁免 | 2026-01-15 | 2026-02-16 |
| 2.2.4 | SC096 | 豁免 DNSSEC 驗證記錄的要求 | 2026-01-14 | 2026-02-17 |
| 2.2.5 | SC097 | 淘汰所有還在使用 SHA-1 簽章的憑證與 CRL | 2026-02-24 | 2026-02-25 |
| 2.2.6 | SC095 | 2025 整理 | 2026-02-27 | 2026-03-31 |
| 2.2.7 | SC099 | 改進驗證方法的記錄方式 | 2026-04-18 | 2026-05-19 |
| 2.2.8 | SC098 | 處理 RFC 8657 的 CAA 參數 | 2026-05-13 | 2026-06-16 |
| 2.2.9 | SC101 | 明定經授權網域名稱（ADN） | 2026-07-02 | 2026-08-06 |
| 2.3.0 | SC100 | DNSSEC 之釐清與整合 | 2026-08-06 | 2026-09-07 |

* 生效日期（Effective Date）及其他相關實施日期

### 1.2.2 相關日期

| 實施日期 | 章節 | 摘要說明（詳情請參閱章節全文） |
|---|---|---|
| 2025-01-15 | 4.9.9 | 用戶憑證（Subscriber Certificate）的 OCSP 回應**應（MUST）**於簽發後 15 分鐘內可用。 |
| 2025-01-15 | 3.2.2.4 | CA **不得（MUST NOT）**依賴 HTTPS 網站來識別網域名稱聯絡人（Domain Contact）資訊。CA **應（MUST）**依賴 IANA 來源識別網域名稱聯絡人資訊。 |
| 2025-03-15 | 4.3.1.2 | CA **應（SHALL）**實施 Linting 流程，以測試待簽發憑證（to-be-issued Certificate）與本文件之間的技術符合性。 |
| 2025-03-15 | 8.7 | CA **宜（SHOULD）**採用 Linting 流程，對內部稽核（Self-Audits）所選定之樣本集中的已簽發憑證進行技術準確度測試。 |
| 2025-03-15 | 3.2.2.9 | CA **應（MUST）**在指定的情況下，從多個網路視角（Network Perspectives）佐證網域驗證（Domain Validation）與 CAA 檢查的結果。 |
| 2025-07-15 | 3.2.2.4 | CA **不得（MUST NOT）**依賴第 3.2.2.4.2 節與第 3.2.2.4.15 節的方法來簽發用戶憑證。 |
| 2025-12-01 | 5.7.1.2 | CA **應（SHALL）**於其 CPS 或合併式 CP/CPS 的第 5.7.1 節中聲明其大規模廢止計畫（Mass Revocation Plan）、演練及持續改進。 |
| 2026-03-15 | 3.2.2.4 | 針對由主要網路視角（Primary Network Perspective）執行之網域授權或控管權驗證相關的所有 DNS 查詢，均**應（MUST）**執行 DNSSEC 驗證。 |
| 2026-03-15 | 3.2.2.4 | CA **不得（MUST NOT）**利用內部政策，針對任何與網域授權或控管權驗證相關的 DNS 查詢，停用其 DNSSEC 驗證。 |
| 2026-03-15 | 3.2.2.4 | CA **不得（MUST NOT）**依賴第 3.2.2.4.8 節的方法來簽發用戶憑證。 |
| 2026-03-15 | 4.2.2.2.2 | 針對由主要網路視角（Primary Network Perspective）執行之與 CAA 紀錄檢查相關的所有 DNS 查詢，均**應（MUST）**執行 DNSSEC 驗證。 |
| 2026-03-15 | 4.2.2.2.4 | CA **不得（MUST NOT）**利用內部政策，針對任何與 CAA 紀錄檢查相關的 DNS 查詢，停用其 DNSSEC 驗證。 |
| 2026-03-15 | 4.2.2.2.5 | 由主要網路視角（Primary Network Perspective）觀察到的 DNSSEC 驗證錯誤（例如 SERVFAIL），**不得（MUST NOT）**被視為許可簽發之依據。 |
| 2026-03-15 | 4.2.1 | 可重複使用主體識別資訊（Subject Identity Information）已驗證資料的最長期限為 398 日。 |
| 2026-03-15 | 4.2.1 | 可重複使用網域名稱（Domain Name）與 IP 位址（IP Address）已驗證資料的最長期限為 200 日。 |
| 2026-03-15 | 4.2.2 | CA **不得（SHALL NOT）**簽發以 IP 反向區域後綴（IP Reverse Zone Suffix）結尾之網域名稱的憑證。 |

| 實施日期 | 章節 | 摘要說明（詳情請參閱章節全文） |
| --- | --- | --- |
| 2026-03-15 | 6.3.2 | 用戶憑證的最長有效期（Validity Period）為 200 日。 |
| 2026-03-15 | 7.1.2.4 | CA **不得（MUST NOT）**使用預簽憑證簽章憑證機構（Precertificate Signing CA）來簽發預簽憑證（Precertificate）。CA **不得（MUST NOT）**使用第 7.1.2.4 節所規範的受技術約束之預簽憑證簽章憑證機構憑證剖繪（Technically Constrained Precertificate Signing CA Certificate Profile）來簽發憑證。 |
| 2026-07-15 | 5.4.1 | 驗證活動的稽核紀錄（Audit logs）**應（MUST）**包含特定資訊。 |
| 2026-09-15 | 7.1.3.2.1 | 淘汰（Sunset）所有還在使用 SHA-1 簽章的憑證與 CRL。 |
| 2026-11-15 | 3.2.2.4 | 經授權網域名稱（Authorization Domain Name，ADN）必須依所使用的驗證方法決定。 |
| 2027-03-15 | 3.2.2.4 與 3.2.2.5 | CA **不得（MUST NOT）**依賴第 3.2.2.4.16 節、第 3.2.2.4.17 節、第 3.2.2.5.2 節與第 3.2.2.5.5 節的方法來簽發用戶憑證。 |
| 2027-03-15 | 3.2.2.5.3 | CA **不得（MUST NOT）**依賴第 3.2.2.5.3 節的方法來簽發用戶憑證。 |
| 2027-03-15 | 4.2.1 | 可重複使用網域名稱與 IP 位址已驗證資料的最長期限為 100 日。 |
| 2027-03-15 | 6.3.2 | 用戶憑證的最長有效期為 100 日。 |
| 2027-03-15 | 4.2.2.1.2 | CA **應（MUST）**依 RFC 8657 規定處理 `accounturi` 與 `validationmethods` 參數。 |
| 2027-03-15 | 4.2.2.1.2 | 若 CA 未依 RFC 8555 所述，以 ACME Account URL 識別憑證用戶的帳號，CA **應（MUST）**於其憑證政策（CP）及／或憑證實務作業基準（CPS）第 4.2 節中定義其所支援的 `accounturi` 格式，並**宜（SHOULD）**遵循 RFC 7565 所定義的 `acct` URI scheme。 |
| 2028-03-15 | 3.2.2.4 與 3.2.2.5 | CA **不得（MUST NOT）**依賴第 3.2.2.4.4 節、第 3.2.2.4.13 節與第 3.2.2.4.14 節的方法來簽發用戶憑證。 |
| 2029-03-15 | 4.2.1 | 可重複使用網域名稱與 IP 位址已驗證資料的最長期限為 10 日。 |
| 2029-03-15 | 6.3.2 | 用戶憑證的最長有效期為 47 日。 |

## 1.3 PKI 參與者

CA/Browser Forum 係一自願性組織（voluntary organization），由憑證機構（Certification Authorities）以及網際網路瀏覽器供應商與其他作為信賴憑證者（Relying-party）的軟體應用程式供應商所組成。

### 1.3.1 憑證機構（CA）

憑證機構（Certification Authority，CA）之定義見第 1.6 節。CA/Browser Forum 目前的 CA 會員名單如以下網址：https://cabforum.org/members。

### 1.3.2 註冊中心（RA）

除第 3.2.2.4 節、第 3.2.2.5 節 及（自 2026-03-15 起生效）第 3.2.2.8 節之要求外，CA **得（MAY）**將第 3.2 節規定之全部或任何部分要求，委派給受委任第三方（Delegated Third Party）執行，前提是整體流程完全符合第 3.2 節所有要求。

於 CA 授權受委任第三方執行受委託作業（delegated function）之前，CA **應（SHALL）**透過契約要求受委任第三方：

1. 於受委託作業適用時，應符合第 5.3.1 節所規定之資格要求；
2. 依第 5.5.2 節保留文件；
3. 遵守本文件中其他適用於受委託作業之規定；以及
4. 遵循
    a. CA 的憑證政策（CP）／憑證實務作業基準（CPS），或
    b. 受委任第三方之作業基準，且 CA 已驗證其遵循本文件要求。

CA **得（MAY）**指定企業註冊中心（Enterprise RA）驗證其所屬組織提出的憑證申請。

CA **不得（SHALL NOT）**接受由企業註冊中心核准的憑證申請，除非符合下列要求：

1. CA **應（SHALL）**確認所申請之完全吻合網域名稱（Fully-Qualified Domain Name，FQDN）位於該企業註冊中心已驗證之網域名稱空間（Domain Namespace）內。
2. 如憑證申請包含非完全吻合網域名稱（FQDN）類型之主體名稱（Subject name），CA **應（SHALL）**確認該名稱為受委任企業之名稱、受委任企業的關係企業（Affiliate）之名稱，或受委任企業係該主體所載名稱之代理人。例如，CA **不得（SHALL NOT）**僅憑企業註冊中心「ABC Co.」之授權而簽發包含主體名稱「XYZ Co.」之憑證，除非兩家公司為關係企業（參見第 3.2 節）或「ABC Co.」係「XYZ Co.」之代理人。無論伴隨申請之主體 FQDN（Subject FQDN）是否屬於「ABC Co.」已註冊域名之網域名稱空間內，上述要求均應適用。

CA **應（SHALL）**透過契約要求該企業註冊中心遵守上述限制，並監督其遵循情形。

### 1.3.3 用戶

依第 1.6.1 節之定義。

在某些情況下，CA 本身會作為申請者（Applicant）或用戶（Subscriber），例如當其產製並保存私密金鑰（Private Key）、申請憑證、證明網域控管權，或為了自身用途取得憑證時。

### 1.3.4 信賴憑證者

「信賴憑證者（Relying Party）」與「應用軟體供應商（Application Software Supplier）」之定義見第 1.6.1 節。CA/Browser Forum 現任會員中屬於應用軟體供應商者，名單如以下網址：https://cabforum.org/members。

### 1.3.5 其他參與者
曾參與本文件制定之其他團體包括 AICPA／CICA 之「WebTrust for Certification Authorities」工作小組與 ETSI ESI。此等團體的參與並不代表其對最終成果之背書、推薦或核可。

## 1.4 憑證用途

### 1.4.1 憑證適用範圍
本文件之主要目的為促進安全且有效之電子通訊，並回應使用者對憑證可信度之疑慮。本文件亦提供使用者相關資訊，協助其於信賴憑證時做出適當判斷。

### 1.4.2 憑證禁止事項
不作規定。

## 1.5 政策管理
《公開信賴 TLS 伺服器憑證簽發與管理之基本要求》（Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates）載明 CA/Browser Forum 所訂定之準則，供憑證機構於簽發、維護及廢止公開信賴 TLS 伺服器憑證時使用。本文件得依 CA/Browser Forum 所採行之程序，適時辦理修訂。鑑於本文件的主要受益者之一為終端使用者，CA/Browser Forum 公開歡迎任何人以電子郵件向 CA/Browser Forum 提出建議（電子郵件地址為 questions@cabforum.org）。CA/Browser Forum 成員重視各界所提出之意見，不論其來源為何，均將予以審慎考量。

### 1.5.1 文件管理單位
不作規定。

### 1.5.2 聯絡資料
CA/Browser Forum 聯絡資訊如以下網址：https://cabforum.org/leadership/。於憑證機構（Certification Authority，CA）的憑證實務作業基準（CPS）本節內容中，CA 應提供連線至網頁之連結或電子郵件地址，以供聯繫負責 CA 營運之人員。

### 1.5.3 憑證實務作業基準（CPS）文件之審定者
不作規定。

### 1.5.4 憑證實務作業基準（CPS）文件之核准程序
不作規定。

## 1.6 名詞定義及縮寫

CA/Browser Forum《網路與憑證系統安全要求》（Network and Certificate System Security Requirements）所載之定義，以引用方式納入本文件，其內容視同已全文載明於本文件。

### 1.6.1 名詞定義

**關係企業/關係組織（Affiliate）**：係指公司、合夥企業、合資企業或其他實體，且該實體控制他實體、受他實體控制，或與他實體受共同控制；亦指政府機關、部門、各級自治團體，或在政府機關直接控制下運作之任何實體。

**申請者（Applicant）**：係指申請（或尋求展期）憑證之自然人或法人（Legal Entity）。憑證一旦核發，申請者即稱為用戶（Subscriber）。針對核發給裝置之憑證，申請者係指控管或營運該憑證所載裝置之實體，縱使該憑證申請實際上是由該裝置所發出。

**申請者代表（Applicant Representative）**：係指本身為申請者、受雇於申請者，或經明確授權可代表申請者之代理人的自然人或 Human Sponsor（資產保管人），且符合下列任一項或多項條件：

i. 代表申請者簽署並提出、或同意憑證申請；及／或

ii. 代表申請者簽署並提出用戶協議（Subscriber Agreement）；及／或

iii. 當申請者為憑證機構之關係企業或即為憑證機構本身時，代表申請者確認使用條款（Terms of Use）。

**應用軟體供應商（Application Software Supplier）**：提供網際網路瀏覽器軟體或其他作為信賴憑證者的應用軟體之供應商，其軟體會顯示或使用憑證，並內建根憑證（Root Certificates）。

**證明信函（Attestation Letter）**：係指由會計師、律師、政府官員或依慣例在此類資訊上具備可信度之可靠第三方所撰寫，用以證實主體資訊（Subject Information）為正確之信函。

**稽核期間（Audit Period）**：於一段期間之稽核（period-of-time audit）中，稽核者於其委任案件中所涵蓋之作業首日（開始）至最後一日（結束）之期間。（此期間不等同稽核者在憑證機構實地稽核期間。）稽核期間之涵蓋規則與最長期限見第 8.1 節。

**稽核報告（Audit Report）**：由合格稽核業者（Qualified Auditor）所出具之報告，用以說明被稽核實體之流程與控管措施是否遵循本文件要求規定的強制性規定之意見。

**經授權網域名稱（ADN, Authorization Domain Name）**：係指用以對指定之完全吻合網域名稱（FQDN）或萬用網域名稱（Wildcard Domain Name）執行網域授權或控管權驗證之 FQDN。

**授權連接埠（Authorized Ports）**：下列連接埠之一：80（http）、443（https）、25（smtp）、22（ssh）。

**基礎網域名稱（Base Domain Name）**：於指定之完全吻合網域名稱（FQDN）中，位於註冊表控制網域或公開字尾（registry-controlled or public suffix）左方第一個網域名稱節點（Domain Name node），加上該註冊表控制網域或公開字尾之部分（例如「example.co.uk」或「example.com」）。若 FQDN 最右端之網域名稱節點在其註冊協議（registry agreement）中具備 ICANN 規格 13（Specification 13）之通用頂級網域名稱（gTLD），則該 gTLD 本身可被當作基礎網域名稱。

**授權憑證機構簽發憑證（CAA）**：節錄自 RFC 8659：「授權憑證機構簽發憑證（Certification Authority Authorization，CAA） DNS 資源紀錄（DNS Resource Record）允許 DNS 網域名稱持有人指定一個或多個憑證機構（CA）取得授權幫該網域名稱簽發憑證。CAA 資源紀錄允許公開 CA 實施額外的控管措施，以降低非預期憑證誤發之風險。」

**CA 金鑰對（CA Key Pair）**：其公開金鑰資訊被記載於一個或多個憑證機構的根憑證及／或下屬憑證機構憑證中的 Subject Public Key Info 欄位之金鑰對。

**憑證（Certificate）**：係指以數位簽章繫結公開金鑰與特定身分之電子文件。

**憑證資料（Certificate Data）**：由憑證機構持有、控管或可存取之憑證申請及其相關資料（無論取自申請者或其他來源）。

**憑證管理流程（Certificate Management Process）**：憑證機構用於驗證憑證資料、簽發憑證、維護儲存庫與廢止憑證所涉及之流程、實務與程序，包括金鑰、軟體與硬體之使用。

**憑證政策（CP, Certificate Policy）**：指一套規則，用以說明特定憑證對於特定社群及／或具有共同安全需求之公開金鑰基礎建設（PKI）運用的適用性。

**憑證問題報告（Certificate Problem Report）**：針對疑似金鑰遭破解（Key Compromise）、憑證遭誤用（misuse）或其他與憑證相關之詐騙、破解、濫用或不當行為之投訴。

**憑證剖繪（Certificate Profile）**：係指一組文件或檔案，用以定義憑證內容與憑證擴充欄位，例如憑證機構（CA）之憑證實務作業基準中的某一章節或 CA 軟體所使用的憑證模板檔案。

**憑證廢止清冊（CRL, Certificate Revocation List）**：由簽發憑證之憑證機構建立並以數位方式簽章，且定期更新時間戳記之已廢止憑證清單。

**憑證機構（CA, Certification Authority）**：負責憑證之建立、簽發、廢止與管理之組織。本詞同時適用根憑證機構（Root CA）與下屬憑證機構（Subordinate CA）。

**憑證實務作業基準（CPS, Certification Practice Statement）**：構成憑證建立、簽發、管理及運用之治理架構的若干文件之一。

**控制（Control）**：「控制」（及其相關用語「受其控制（controlled by）」與「與其受共同控制（under common control with）），係指直接或間接擁有下列權力之一：(1) 主導該實體之經營、人事、財務或計畫；(2) 控制過半董事之選任；或 (3) 表決權依該實體設立地或註冊地管轄法律中構成「控制」所需之表決權股份比例，但無論如何不得少於 10%。

**國家（Country）**：聯合國會員國，**或（OR）**經至少兩個聯合國會員國承認為主權國家（Sovereign State）之地理區域。

**交互認證之下屬憑證機構憑證（Cross-Certified Subordinate CA Certificate）**：於兩個憑證機構之間建立信賴關係的憑證。

**密碼學安全偽亂數產生器（CSPRNG）**：供密碼學系統使用之亂數產生器。

**受委任第三方（Delegated Third Party）**：非屬憑證機構（CA）之自然人或法人（Legal Entity），獲 CA 授權執行或履行本文件所列之一項或多項 CA 要求事項，以協助憑證管理流程，且其相關活動未納入 CA 稽核適用範圍。

**DNS CAA 電子郵件聯絡人（DNS CAA Email Contact）**：附錄 A.1.1所定義的電子郵件地址。

**DNS CAA 電話聯絡人（DNS CAA Phone Contact）**：附錄 A.1.2所定義的電話號碼。

**DNS TXT 紀錄電子郵件聯絡人（DNS TXT Record Email Contact）**：附錄 A.2.1所定義的電子郵件地址。

**DNS TXT 紀錄電話聯絡人（DNS TXT Record Phone Contact）**：附錄 A.2.2所定義的電話號碼。

**網域標籤（Domain Label）**：節錄自 RFC 8499：「由零個或多個位元組（octet）依序組合而成，用以構成網域名稱的一部分。以圖論（Graph theory）表示時，網域標籤用於識別所有可能的網域名稱所構成之圖形結構中的一個節點。」

**網域名稱（Domain Name）**：由一個或多個網域標籤（Domain Label）依序組合而成，並被當作網域名稱系統（DNS）中的一個節點。

**網域名稱空間（Domain Namespace）**：網域名稱系統中（DNS）中，一個節點轄下之所有可能的網域名稱之集合。

**網域名稱註冊人（Domain Name Registrant）**：有時被稱為網域名稱的「擁有者（owner）」，但更精確而言，係指個人或實體被網域名稱註冊商（Domain Name Registrar）註冊為具有權利控管網域名稱使用方式之個人或實體，例如於 WHOIS 查詢或網域名稱註冊商資料中被列在「Registrant」之自然人或法人。

**網域名稱註冊商（Domain Name Registrar）**：經下列機構授權或與其簽訂協議，而辦理網域名稱註冊之個人或實體：

i. 網際網路名稱與號碼指配機構（ICANN）；

ii. 國家級網域名稱主管機關或註冊管理機構（authority/registry）；或

iii. 網路資訊中心（Network Information Center, NIC）（包括其關係企業、承包商、受委任單位、繼承人或受讓人）。

**企業註冊中心（Enterprise RA）**：與憑證機構無關聯之組織的員工或代理人，獲授權向該組織核准憑證之簽發。

**到期日（Expiry Date）**：憑證中「Not After」欄位之日期，定義憑證有效期之終止。

**完全吻合網域名稱（FQDN, Fully-Qualified Domain Name）**：指包含其所有於DNS上層節點之網域標籤的完整網域名稱。

**政府機關（Government Entity）**：由政府設立或運作之法人、機關、部門、部會、分支機構或其他類似之政府組織，以及該國轄下各級地方自治團體（如州、省、市、縣等）。

**高風險憑證申請（High Risk Certificate Request）**：指憑證機構（CA）依內部準則及所維護的資料庫內容，將某一憑證申請標示為須額外審查之申請。相關準則及資料庫收錄容易遭用於網路釣魚或其他詐欺用途之主體名稱、曾出現於遭拒絕之憑證申請或已廢止憑證的主體名稱、被列在 Miller Smiles Phishing List 或 Google Safe Browsing List 中之網域名稱，或 CA 依其自身風險減輕準則所識別之名稱。

**內部名稱（Internal Name）**：指憑證之 Common Name 或 Subject Alternative Name 欄位中的字串（非 IP 位址），由於其並非使用登記於 IANA Root Zone Database 的頂級網域名稱（Top-Level Domain, TLD）作為結尾，故於憑證簽發時無法在公開 DNS 中驗證其具有全球唯一性。

**IP 位址（IP Address）**：指配給使用網際網路協定（Internet Protocol, IP）進行通訊之裝置的 32 位元或 128 位元數值。

**IP 位址聯絡人（IP Address Contact）**：經 IP 位址註冊管理機構登記為有權控管一個或多個 IP 位址使用方式之個人或實體。

**IP 位址註冊管理機構（IP Address Registration Authority）**：網際網路號碼分配機構（IANA）或區域網際網路註冊管理機構（RIPE、APNIC、ARIN、AfriNIC、LACNIC）。

**IP 反向區域後綴（IP Reverse Zone Suffix）**：由網域標籤「in-addr.arpa」或「ip6.arpa」所構成之兩個完全吻合網域名稱（FQDN）之一。此二個 FQDN 分別作為網際網路協定第 4 版（IPv4）及第 6 版（IPv6）反向對應（Reverse Mapping）命名空間之根節點。其中，「in-addr.arpa」為 IPv4 反向對應命名空間之根節點，「ip6.arpa」則為 IPv6 反向對應命名空間之根節點。

**簽發憑證機構（Issuing CA）**：對一張憑證而言，即簽發該憑證之憑證機構（CA）。可以是根憑證機構（Root CA）或下屬憑證機構（Subordinate CA）。

**金鑰遭破解（Key Compromise）**：當私密金鑰的數值洩漏給未經授權之人士，或未經授權之人士得以存取該私密金鑰時，即稱該私密金鑰遭破解。

**金鑰產製腳本（Key Generation Script）**：用於產製憑證機構（CA）金鑰對之書面程序計畫。

**金鑰對（Key Pair）**：私密金鑰與其對應之公開金鑰。

**LDH 標籤（LDH Label）**：節錄自 RFC 5890：「由 ASCII 字母、數字與連字號組成之字串，且連字號不得出現於字串開頭或結尾。如同所有 DNS 標籤，其總長度不得超過 63 個位元組（octet）。」

**法人（Legal Entity）**：於一國法律制度中具合法地位之社團、公司、合夥、獨資、信託、政府機關或其他實體。

**Linting（語法檢查）**：針對預簽憑證（RFC 6962）、憑證、憑證廢止清冊（CRL）或線上憑證狀態協定（OCSP）回應等已完成數位簽章之資料，或待簽章的資料物件，例如 `tbsCertificate`（如 RFC 5280, 第 4.1.1.1 節 所述），檢查其內容是否符合本文件所定義之剖繪及要求的流程。

**多視角簽發佐證（Multi-Perspective Issuance Corroboration）**：於憑證簽發前，由其他網路視角（Network Perspectives）佐證主要網路視角（Primary Network Perspective）在網域驗證及 CAA 檢查時所做判定之流程。

**網路視角（Network Perspective）**：與多視角簽發佐證（Multi-Perspective Issuance Corroboration）相關。指用於發送網域控管權驗證（Domain Control Validation）方法及／或 CAA 檢查相關之對外網際網路流量的系統（例如雲端代管伺服器的執行個體），或網路元件的組合（例如 VPN 及其相關基礎設施）。網路視角之位置，通常係指未封裝之對外網際網路流量首次交接給提供該視角網際網路連線之網路基礎設施的地點。

**非保留 LDH 標籤（Non-Reserved LDH Label）**：節錄自 RFC 5890：「第三與第四個字元位置不含『`--`』之有效 LDH 標籤集合。」

**物件識別碼（OID, Object Identifier）**：於國際標準化組織（ISO）適用標準下，為特定物件或物件類別所註冊之唯一英數字或數字識別碼。

**OCSP 回應伺服器（OCSP Responder）**：係指在 CA 授權下營運的線上伺服器，並連線至其憑證儲存庫，用以處理憑證狀態之查詢請求。亦參見「線上憑證狀態協定（OCSP）」之定義。

**Onion 網域名稱（Onion Domain Name）**：以 RFC 7686 所定義之「.onion」特殊用途網域名稱（Special-Use Domain Name）結尾之完全吻合網域名稱（FQDN）。例如，`2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion` 為 Onion 網域名稱，反之，`torproject.org` 則非 Onion 網域名稱。

**線上憑證狀態協定（OCSP, Online Certificate Status Protocol）**：係一種線上憑證檢查協定，用以使作為信賴憑證者的應用軟體得以判定某張憑證之狀態。亦參見「OCSP 回應伺服器」之定義。

**母公司（Parent Company）**：控制子公司（Subsidiary Company）之公司。

**預告禁用（Pending Prohibition）**：指極不鼓勵使用描述中有此標籤之行為，因該行為已被規劃予以廢止（Deprecated），且未來極可能被指定為**不得（MUST NOT）**使用。

**持久性網域控管權 TXT 紀錄（Persistent DCV TXT Record）**：依第 3.2.2.4.22 節規定，用於識別申請者之 DNS TXT 紀錄。

**預簽憑證（Precertificate）**：依 RFC 6962 之定義，可提出至憑證透明度（Certificate Transparency）記錄系統之已簽章資料結構，且包含關鍵性 poison 擴充欄位（OID：1.3.6.1.4.1.11129.2.4.3）。

**主要網路視角（Primary Network Perspective）**：憑證機構（CA）用以判定下列事項之網路視角（1）CA 是否有權限為所申請之網域或 IP 位址簽發憑證，以及（2）申請者是否具有相關權限，及／或獲得所申請網域或 IP 位址之網域授權或控管權。

**私密金鑰（Private Key）**：金鑰對中由持有人保密持有之金鑰，用以建立數位簽章及／或解密其對應公開金鑰所加密之電子紀錄或檔案。

**公開金鑰（Public Key）**：係指金鑰對中，私密金鑰持有人可對外公開之對應金鑰。信賴憑證者用以驗證持有人以對應私密金鑰所建立之數位簽章，及／或用以將訊息加密，使加密訊息僅能由持有人以對應私密金鑰解密。

**公開金鑰基礎建設（PKI, Public Key Infrastructure）**：基於公開金鑰密碼學之硬體、軟體、人員、程序、規範、政策與義務之集合體，被用以協助憑證與金鑰之可信賴建立、簽發、管理及使用。

**公開信賴憑證（Publicly-Trusted Certificate）**：因其對應之根憑證，以信賴根源（Trust Anchor）之形式配發於廣泛使用之應用軟體中，進而受到信任之憑證。

**P-Label**：係指自第五個字元位置起，包含 Punycode 演算法有效輸出字串（如 RFC 3492, 第 6.3 節 所定義）之 XN-Label。

**合格稽核業者（Qualified Auditor）**：符合第 8.2 節規定之稽核資格所要求之自然人或法人。

**隨機值（Random Value）**：憑證機構提供予申請者的指定數值，其具備至少 112 位元之亂度（entropy，資訊熵）。

**已註冊網域名稱（Registered Domain Name）**：已向網域名稱註冊商登記的網域名稱。

**註冊中心（RA, Registration Authority）**：負責憑證主體之識別與鑑別，但本身非憑證機構（CA），且不簽署或簽發憑證之任何法人。註冊中心（RA）得協助憑證申請流程、憑證廢止流程，或同時協助兩者。當「RA」作為形容詞用以描述角色或功能時，並不必然表示其為獨立機構，亦可能為 CA 之一部分。

**可靠資料來源（Reliable Data Source）**：用以驗證主體識別資訊（Subject Identity Information）之識別文件或資料來源，為商業界及政府機關普遍認可之可靠來源，且係由第三方基於憑證申請以外之目的所建立。

**可靠通訊方式（Reliable Method of Communication）**：以申請者代表以外之來源完成驗證的通訊方式，例如信箱／快遞地址、電話號碼或電子郵件地址。

**信賴憑證者（Relying Party）**：信賴（使用）有效憑證之任何自然人或法人。當應用軟體供應商所發布之軟體僅顯示憑證相關資訊時，該供應商不視為信賴憑證者。

**儲存庫（Repository）**：提供公開揭露之 PKI 治理文件（例如憑證政策與憑證實務作業基準）及憑證狀態資訊之線上資料庫；憑證狀態資訊可用 CRL 或 OCSP 回應之形式提供。

**請求符記（Request Token）**：依憑證機構（CA）指定方法所產生之值，用以將控管權證明與憑證申請繫結起來。CA **宜（SHOULD）**於其憑證實務作業基準（或憑證實務作業基準明確引用之文件）中定義其接受之請求符記格式與產生方法。

請求符記**應（SHALL）**加進憑證請求所使用之金鑰。

請求符記**得（MAY）**包含時間戳記，以標示其建立時間。

請求符記**得（MAY）**包含其他資訊，以確保其唯一性。

包含時間戳記之請求符記，其有效期自建立起**應（SHALL）**不超過 30 日。

包含時間戳記之請求符記，若其時間戳記為未來時間，**應（SHALL）**視為無效。

不含時間戳記之請求符記僅供單次使用，CA **不得（SHALL NOT）**於後續驗證中重複使用（re-use）。

該繫結機制**應（SHALL）**至少使用與憑證請求簽章所用之同等強度數位簽章演算法或密碼學雜湊演算法。

**註**：請求符記之範例，包括但不限於：

i. 公開金鑰之雜湊；或

ii. Subject Public Key Info [X.509] 之雜湊；或

iii. PKCS#10 憑證請求檔（CSR）之雜湊。

請求符記亦可與時間戳記或其他資料串連。若 CA 希望一律以 PKCS#10 憑證請求檔（CSR）之雜湊作為請求符記，且不欲加進時間戳記、又欲允許憑證金鑰對重複使用，則申請者於使用 OpenSSL 建立憑證請求檔時可加入挑戰密碼（Challenge Password），以確保即使後續請求檔使用相同之主體與金鑰，仍能維持其唯一性。

**註**：以下這個簡單的 shell 指令會產生一個包含時間戳記與憑證請求檔（CSR）雜湊的請求符記（Request Token）：`echo `date -u +%Y%m%d%H%M` `sha256sum <r2.csr` \| sed "s/[ -]//g"` 其指令輸出如下：
`201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f`

**所要求的網站內容（Required Website Content）**：指隨機值或請求符記其中之一，連同由憑證機構指定，用以識別用戶唯一性之額外資訊。

**Requirements**：指本文件所載之《基本要求》（Baseline Requirements）；下文視語境以「本文件」（指文件本體）或「本文件要求規定」（指其規範內容）稱之。

**保留 IP 位址（Reserved IP Address）**：下列 IANA 登錄表所列位址區塊（Address Block）中之任一 IPv4 或 IPv6 位址：

https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

**反向區域網域名稱（Reverse Zone Domain Name）**：於 `.arpa` 名稱空間中，對應某 IP 位址之完全吻合網域名稱（FQDN）。此 FQDN 係將 IP 位址轉換為一連串標籤後，附加適用之 IP 反向區域後綴所構成，如 RFC 1035（IPv4 位址）與 RFC 3596（IPv6 位址）所載。

**根憑證機構（Root CA）**：指頂層憑證機構，其根憑證由應用軟體供應商配發，並簽發下屬憑證機構憑證。

**根憑證（Root Certificate）**：根憑證機構所簽發之自簽憑證，用以識別其自身，並協助驗證其對下屬憑證機構簽發之憑證。

**短效期用戶憑證（Short-lived Subscriber Certificate）**：對於 2024-03-15 起至 2026-03-15 前簽發之憑證，指有效期小於或等於 10 日（864,000 秒）之用戶憑證。對於 2026-03-15 起簽發之憑證，指有效期小於或等於 7 日（604,800 秒）之用戶憑證。

**主權國家（Sovereign State）**：自行管理其政府，且不依附或受制於另一政權之國家或國土。

**主體（Subject）**：憑證中被識別為「主體」之自然人、裝置、系統、單位或法人。主體為用戶本身，或受該用戶控管與營運之裝置。

**主體識別資訊（Subject Identity Information）**：用以識別憑證主體的資訊。主體識別資訊不包含 `subjectAltName` 擴充欄位或主體 `commonName` 欄位所列之網域名稱或 IP 位址。

**下屬憑證機構（Subordinate CA）**：其自身憑證由根憑證機構（Root CA）或其他下屬憑證機構所簽章之憑證機構。

**用戶（Subscriber）**：被簽發憑證且受用戶協議（Subscriber Agreement）或使用條款（Terms of Use）約束之自然人或法人。

**用戶協議（Subscriber Agreement）**：憑證機構與申請者／用戶之間的協議，載明雙方之權利義務。

**子公司（Subsidiary Company）**：受母公司控制之公司。

**受技術約束的下屬憑證機構憑證（Technically Constrained Subordinate CA Certificate）**：指依本文件相關憑證剖繪（Certificate Profile）之規定，使用 Extended Key Usage 及／或 Name Constraints 擴充欄位之組合，限制該下屬憑證機構（CA）憑證簽發用戶憑證或其他下屬 CA 憑證之範圍。

**使用條款（Terms of Use）**：當申請者／用戶為憑證機構（CA）之關係企業或 CA 本身時，用以規範依本文件要求規定簽發之憑證的保管與允許用途。

**測試憑證（Test Certificate）**：本詞已不再《基本要求》中使用。

**頂級網域（TLD, Top-Level Domain）**：節錄自 RFC 8499：「頂級網域為根網域下一層之區域，例如『com』或『jp』。」

**可信賴系統（Trustworthy System）**：具有下列性質之電腦硬體、軟體與程序：對於入侵與誤用有合理地保護；提供合理水準之可用性、可靠性與正確運作；合理適當地執行其預定功能；並落實適用的安全政策。

**未註冊網域名稱（Unregistered Domain Name）**：非已註冊網域名稱之網域名稱。

**有效憑證（Valid Certificate）**：通過 RFC 5280 所規定之驗證程序的憑證。

**驗證專員（Validation Specialist）**：執行本文件所規定之資訊驗證作業的人員。

**有效期（Validity Period）**：節錄自 RFC 5280：「自 `notBefore` 至 `notAfter`（含）之期間。」

**WHOIS**：係指透過 RFC 3912 所定義之 WHOIS 協定、RFC 7482 所定義之註冊資料存取協定（RDAP），或者透過 HTTPS 網站，直接從網域名稱註冊商或註冊管理機構取得之資訊。

**萬用網域憑證（Wildcard Certificate）**：在憑證主體別名／主體替代名稱中至少含有一個萬用網域名稱之憑證。

**萬用網域名稱（Wildcard Domain Name）**：以「*.」（U+002A ASTERISK、U+002E FULL STOP）開頭，緊接完全吻合網域名稱之字串。

**XN-Label**：節錄自 RFC 5890：「以前綴『`"xn--"`』（不分大小寫）開頭，且其餘部分遵循 LDH 標籤規則之一類標籤。」

### 1.6.2 縮寫

| 縮寫 | 全稱 |
| --- | --- |
| AICPA | 美國會計師公會（American Institute of Certified Public Accountants） |
| ADN | 經授權網域名稱（Authorization Domain Name） |
| CA | 憑證機構（Certification Authority） |
| CAA | 授權憑證機構簽發憑證（Certification Authority Authorization） |
| ccTLD | 國碼頂級網域名稱（Country Code Top-Level Domain） |
| CICA | 加拿大會計師公會（Canadian Institute of Chartered Accountants） |
| CP | 憑證政策（Certificate Policy） |
| CPS | 憑證實務作業基準（Certification Practice Statement） |
| CRL | 憑證廢止清冊（Certificate Revocation List） |
| DBA | 商業名稱（Doing Business As） |
| DNS | 網域名稱系統（Domain Name System） |
| FIPS | 美國聯邦資訊處理標準（Federal Information Processing Standard） |
| FQDN | 完全吻合網域名稱（Fully-Qualified Domain Name） |
| IM | 即時通訊（Instant Messaging） |
| IANA | 網際網路號碼分配機構（Internet Assigned Numbers Authority） |
| ICANN | 網際網路名稱與號碼指配機構（Internet Corporation for Assigned Names and Numbers） |
| ISO | 國際標準化組織（International Organization for Standardization） |
| NIST | 美國國家標準與技術研究院（National Institute of Standards and Technology） |
| OCSP | 線上憑證狀態協定（Online Certificate Status Protocol） |
| OID | 物件識別碼（Object Identifier） |
| PKI | 公開金鑰基礎建設（Public Key Infrastructure） |
| RA | 註冊中心（Registration Authority） |
| S/MIME | 安全多用途網際網路郵件擴充協定（Secure MIME, Multipurpose Internet Mail Extensions） |
| SSL | 安全通訊端層協定（Secure Sockets Layer） |
| TLS | 傳輸層安全性協定（Transport Layer Security） |

| 縮寫 | 全稱 |
| --- | --- |
| VoIP | 網際網路協定語音傳輸（Voice Over Internet Protocol） |

### 1.6.3 參考資料

ETSI EN 319 403，電子簽章與基礎建設（Electronic Signatures and Infrastructures，ESI）；信賴服務提供者符合性評鑑 - 針對評鑑信賴服務提供者的符合性評鑑機構之要求。

ETSI EN 319 411-1，電子簽章與基礎建設（Electronic Signatures and Infrastructures，ESI）；簽發憑證之信賴服務提供者的政策與安全要求；第 1 部分：一般要求。

FIPS 140-2，聯邦資訊處理標準發行物 - 密碼模組安全要求，美國國家標準與技術研究院資訊技術實驗室，2001 年 5 月 25 日。

FIPS 140-3，聯邦資訊處理標準發行物 - 密碼模組安全要求，美國國家標準與技術研究院資訊技術實驗室，2019 年 3 月 22 日。

FIPS 186-5，聯邦資訊處理標準發行物 - 數位簽章標準（Digital Signature Standard，DSS），美國國家標準與技術研究院資訊技術實驗室，2023 年 2 月。

ISO 21188:2018，金融服務之公開金鑰基礎建設 —— 實務與政策框架。

網路與憑證系統安全要求，1.7 版，可參閱 https://cabforum.org/network-security-requirements/

NIST SP 800-89，數位簽章應用之取得保證性的建議，https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-89.pdf。

RFC 2119，徵求修正意見書：2119， RFC 中用於標示需求層級之關鍵字。S. Bradner，1997 年 3 月。

RFC 3492，徵求修正意見書：3492，Punycode：用於應用程式的國際化網域名稱（IDNA）之 Unicode 的 Bootstring 編碼。A. Costello，2003 年 3 月。

RFC 3647，徵求修正意見書：3647，網際網路 X.509 公開金鑰基礎建設：憑證政策（CP）與憑證實務作業基準（CPS）框架。S. Chokhani 等，2003 年 11 月。

RFC 3912，徵求修正意見書：3912，WHOIS 協定規範。L. Daigle，2004 年 9 月。

RFC 3986，徵求修正意見書：3986，統一資源識別碼（URI）：通用語法。T. Berners-Lee 等，2005 年 1 月。

RFC 4035，徵求修正意見書：4035，DNS 安全性擴充（DNSSEC）之協定修改。R. Arends 等，2005 年 3 月。

RFC 4509，徵求修正意見書：4509，於 DNSSEC 委派簽章（DS）資源紀錄（RR）中使用 SHA-256。W. Hardaker，2006 年 5 月。

RFC 5019，徵求修正意見書：5019，用於高流量環境之輕量級線上憑證狀態協定（OCSP）剖繪檔。A. Deacon 等，2007 年 9 月。

RFC 5155，徵求修正意見書：5155，DNS 安全（DNSSEC）雜湊化的可驗證之不存在性。B. Laurie 等，2008 年 3 月。

RFC 5280，徵求修正意見書：5280，網際網路 X.509 公開金鑰基礎建設：憑證與憑證廢止清冊（CRL）剖繪檔。D. Cooper 等，2008 年 5 月。

RFC 5702，徵求修正意見書：5702，於 DNSSEC 之 DNSKEY 與 RRSIG 資源紀錄中結合 RSA 使用 SHA-2 演算法。J. Jansen，2009 年 10 月。

RFC 5890，徵求修正意見書：5890，應用程式的國際化網域名稱（IDNA）：定義與文件框架。J. Klensin，2010 年 8 月。

RFC 5952，徵求修正意見書：5952，IPv6 位址文本表示法之建議。S. Kawamura 等，2010 年 8 月。

RFC 6840，徵求修正意見書：6840，DNS 安全（DNSSEC）之說明與實作須知。S. Weiler 等，2013 年 2 月。

RFC 6960，徵求修正意見書：6960，X.509 網際網路公開金鑰基礎建設之線上憑證狀態協定 - OCSP。S. Santesson 等，2013 年 6 月。

RFC 6962，徵求修正意見書：6962，憑證透明度（Certificate Transparency）。B. Laurie 等，2013 年 6 月。

RFC 7231，徵求修正意見書：7231，超文本傳輸協定（HTTP/1.1）：語義與內容。R. Fielding 等，2014 年 6 月。

RFC 7482，徵求修正意見書：7482，註冊資料存取協定（RDAP）的查詢格式。A. Newton 等，2015 年 3 月。

RFC 7538，徵求修正意見書：7538，超文本傳輸協定狀態碼 308（永久重定向）。J. Reschke，2015 年 4 月。

RFC 7565，徵求修正意見書：7565，「acct」URI Scheme。P. Saint-Andre，2015 年 5 月。

RFC 8499，徵求修正意見書：8499，DNS 術語。P. Hoffman 等，2019 年 1 月。

RFC 8555，徵求修正意見書：8555，自動憑證更新環境（ACME）。R. Barnes 等，2019 年 3 月。

RFC 8657，徵求修正意見書：8657，用於繫結 Account URI 與自動憑證更新環境（ACME）方法之授權憑證機構簽發憑證（CAA）紀錄的擴充功能。H. Landau 等，2019 年 11 月。

RFC 8659，徵求修正意見書：8659，DNS 授權憑證機構簽發憑證（CAA）的資源紀錄。P. Hallam-Baker 等，2019 年 11 月。

RFC 8738，徵求修正意見書：8738，自動憑證更新環境（ACME）之 IP 識別字驗證擴充欄位。R.B.Shoemaker 編，2020 年 2 月。

RFC 8954，徵求修正意見書：8954，線上憑證狀態協定（OCSP）之 Nonce 擴充欄位。M. Sahni 編，2020 年 11 月。

RFC 9082，徵求修正意見書：9082，註冊資料存取協定（RDAP）的查詢格式。S. Hollenbeck、A. Newton 等，2021 年 6 月。

WebTrust 憑證機構稽核，SSL 基本要求與網路安全，可參閱 https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria。

WebTrust 憑證機構原則與準則 – SSL 基本要求。

X.509，ITU-T 建議書 X.509 (08/2005) | ISO/IEC 9594-8:2005，資訊技術 – 開放系統之連接 – 目錄：公開金鑰與屬性憑證框架。

### 1.6.4 慣例

本文件中的關鍵字「**應（MUST）**」、「**不得（MUST NOT）**」、「**必要（REQUIRED）**」、「**應（SHALL）**」、「**不得（SHALL NOT）**」、「**宜（SHOULD）**」、「**不宜（SHOULD NOT）**」、「**建議（RECOMMENDED）**」、「**得（MAY）**」及「**選用（OPTIONAL）**」應依據 RFC 2119 解釋。

按照慣例，本文件在列出生效要求（例如日期）時省略時間與時區。除非另有明確說明，否則日期與相關時間應為 00:00:00 UTC。

---

# 2 資訊公佈與儲存庫責任

## 2.1 儲存庫

憑證機構（Certification Authority，CA）**應（SHALL）**依照本政策提供下屬憑證（Subordinate Certificates）與用戶憑證（Subscriber Certificates）的廢止（revocation）資訊。

## 2.2 資訊之公佈

CA **應（SHALL）**透過適當且易於存取的線上管道（online means），提供每週 7 天、每天 24 小時（24x7）之憑證政策（CP）及／或憑證實務作業基準（CPS）的公開揭露。CA **應（SHALL）**於 CA 所選稽核架構（audit scheme）的要求範圍內，對外公開其 CA 業務作業基準（CA business practices）（參見第 8.4

節）。

CA **應（SHALL）**制定、實施、落實憑證政策（CP）及／或憑證實務作業基準（CPS），且至少每 366 日更新一次；其內容詳細描述 CA 如何實作最新版之本文件要求規定。

憑證政策（CP）及／或憑證實務作業基準（CPS）**應（MUST）**依據 RFC 3647 規定之架構撰寫，且**應（MUST）**包含 RFC 3647 要求的所有內容。

CA **應（SHALL）**公開實行（give effect to）本文件要求規定，並聲明（represent）其將遵守最新版本之規定。CA **得（MAY）**將本文件要求規定直接納入（incorporating）其憑證政策（CP）及／或憑證實務作業基準（CPS），或採用如下之聲明條款以引用方式（by reference）納入其中以滿足要求（該條款**應（MUST）**包含本《基本要求》官方版本之連結）：

> “
>
> 【CA名稱】遵循 https://www.cabforum.org 所發布之《公開信賴 TLS 伺服器憑證簽發與管理之基本要求》（Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates）之現行版本規定。若本文件與上述《基本要求》有任何不一致（inconsistency）之處，應優先適用（take precedence）《基本要求》之規定。

CA **應（SHALL）**架設測試網頁，以允許應用軟體供應商（Application Software Suppliers）使用憑證鏈串鏈至（chain up to）各自的公開信賴根憑證（Publicly Trusted Root Certificate）之用戶憑證來測試其軟體。CA 至少**應（SHALL）**架設使用下列狀態之用戶憑證的獨立網頁供測試：

i. 有效（valid），

ii. 廢止（revoked），以及

iii. 過期（expired）。

## 2.3 公佈之時間或頻率

CA **應（SHALL）**制定、實施、落實與每年更新憑證政策（CP）及／或憑證實務作業基準（CPS），其內容詳細描述 CA 如何實作最新版本之《基本要求》規定。CA **應（SHALL）**藉由增加版本號（incrementing the version number）與加入附日期之變更紀錄條目（changelog entry）以表示符合上述要求，即使該文件未進行其他變更亦同。

## 2.4 儲存庫之存取控制

CA 應以唯讀方式公開提供其儲存庫（Repository）。

# 3 識別與鑑別

## 3.1 命名

### 3.1.1 命名種類

### 3.1.2 命名須有意義

### 3.1.3 用戶之匿名或假名

### 3.1.4 各種命名形式之解釋規則

### 3.1.5 命名之獨特性

### 3.1.6 商標之辨識、鑑別及角色

## 3.2 初始身分驗證

### 3.2.1 證明持有私密金鑰之方式

### 3.2.2 組織與網域身分之鑑別

若申請者（Applicant）申請之憑證（Certificate）所包含的主體識別資訊（Subject Identity Information）僅由 `countryName` 欄位組成，則憑證機構（Certification Authority，CA）**應（SHALL）**使用符合第 3.2.2.3 節要求、且已載明於該 CA 之憑證政策（Certificate Policy，CP）及／或憑證實務作業基準（Certification Practice Statement，CPS）中的驗證流程，以驗證主體（Subject）與所屬之國家。若申請者申請之憑證包含 `countryName` 欄位及其他主體識別資訊，則 CA **應（SHALL）**使用符合本文件第 3.2.2.1 節要求、且已載明於該 CA 的憑證政策（CP）及／或憑證實務作業基準（CPS）中的驗證流程，驗證申請者之身分，以及申請者代表（Applicant Representative）所提出之憑證申請的真實性。CA **應（SHALL）**檢查本節所依據之任何文件是否經過竄改或偽造。

#### 3.2.2.1 組織身分之識別

若主體識別資訊（Subject Identity Information）包含組織名稱或地址，憑證機構（Certification Authority，CA）**應（SHALL）**驗證該組織身分與地址，且該地址應為申請者（Applicant）之登記地或營運地址。CA **應（SHALL）**透過下列至少一種方法所提供之文件或通訊往來紀錄，以驗證申請者的身分與地址：

1. 申請者合法設立、存續或獲得認許之所在地主管機關；
2. 定期更新且被視為可靠資料來源（Reliable Data Source）之第三方資料庫；
3. 由 CA 或擔任 CA 代理人之第三方進行實地訪查；或
4. 證明信函（Attestation Letter）。

CA **得（MAY）**使用以上第 1 至 4 項所述之相同文件或聯絡方式，同時驗證申請者的身分與地址。

或者，CA **得（MAY）**透過公用事業費用帳單（如水電瓦斯費）、銀行對帳單、信用卡帳單、政府核發之稅務證明文件，及其他經 CA 認定為可靠的身分證明文件，以驗證申請者之地址（但不包括申請者之身分）。

#### 3.2.2.2 DBA／商業名稱

若主體識別資訊（Subject Identity Information）包含 DBA 或商業名稱，憑證機構（Certification Authority，CA）**應（SHALL）**透過以下至少一種方法，驗證申請者（Applicant）具有使用該 DBA／商業名稱之權利：

1. 申請者合法設立、存續或獲得認許之所在地主管機關所提供的文件或與該機關通訊往來之紀錄；
2. 可靠資料來源（Reliable Data Source）；
3. 與負責管理 DBA 或商業名稱之主管機關進行通訊往來；
4. 檢附證明文件的證明信函（Attestation Letter）；或
5. 公用事業費用帳單（如水電瓦斯費）、銀行對帳單、信用卡帳單、政府核發之稅務證明文件，或其他經 CA 認定為可靠的身分證明文件。

#### 3.2.2.3 驗證所屬國家

若存在 `subject:countryName` 欄位，則憑證機構（Certification Authority，CA）**應（SHALL）**使用以下任一方式，驗證主體（Subject）所屬的國家：

a. 下列任一 IP 位址屬於被指配的國家 IP 位址區段：
   i. 該網站的 IP 位址（以該網站的 DNS 紀錄所指目標為準）或
   ii. 申請者的 IP 位址；
b. 所申請之網域名稱（Domain Name）的國碼頂級網域名稱（ccTLD）；
c. 由網域名稱註冊商（Domain Name Registrar）提供之資訊；或

d. 第 3.2.2.1 節中所定義的方法。

CA **宜（SHOULD）**建立代理伺服器（Proxy Servers）檢查流程，以避免誤信非申請者實際所在地之其他國家的 IP 位址。

### 3.2.2.4 網域授權或控管權之驗證

於 2026-11-15 之前，CA **應（SHALL）**遵守本文件第 3.2.2.4 節（及其各小節）*或*《公開信賴 TLS 伺服器憑證簽發與管理之基本要求》（Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates）第 2.2.7 版第 3.2.2.4 節。自 2026-11-15 起，CA **應（SHALL）**遵守本文件第 3.2.2.4 節。

本節定義憑證機構（Certification Authority，CA）驗證申請者（Applicant）的網域所有權或控管權之允許流程與程序。

CA 替每一個所申請的完全吻合網域名稱（Fully-Qualified Domain Name，FQDN）或萬用網域名稱（Wildcard Domain Name）選擇用於網域驗證的經授權網域名稱（Authorization Domain Name，ADN）時，**應（MUST）**遵從下列流程：

1. 將 A 設為所申請的 FQDN 或萬用網域名稱。
2. 選擇一種驗證方法。若 A 為萬用網域名稱，CA **應（MUST）**選擇下表「萬用網域（Wildcard）」欄中標示「✓」的驗證方法；若 A 為 Onion 網域名稱（Onion Domain Name），CA **應（MUST）**選擇下表「Onion」欄中標示「✓」的驗證方法。
3. 若 A 為 FQDN：
    1. 若該驗證方法於下表「CNAME」欄中標示「✓」，CA **得（MAY）**將 A 替換為對 A 執行 DNS CNAME 查詢所得之結果。本步驟可重複執行。
    2. 若該驗證方法於下表「刪減（Prune）」欄中標示「✓」，且 A 不等於 A 的基礎網域名稱（Base Domain Name），CA **得（MAY）**將 A 替換為自 A 刪除最左側網域標籤（Domain Label）後所得之結果。本步驟可重複執行。
4. 若 A 為萬用網域名稱：
    1. 移除 A 最左端的「*.」。
    2. 若該驗證方法於下表「刪減（Prune）」欄中標示「✓」，且 A 不等於 A 的基礎網域名稱，CA **得（MAY）**將 A 替換為自 A 刪除最左側網域標籤後所得之結果。本步驟可重複執行。
5. 以 A 作為經授權網域名稱（ADN）。

| 驗證方法 | 萬用網域（Wildcard） | 刪減（Prune） | CNAME | Onion |
|---|---|---|---|---|
| 3.2.2.4.4 使用特定格式的地址寄送電子郵件給網域名稱聯絡人 | ✓ | ✓ | ✓ | - |
| 3.2.2.4.7 DNS 變更 | ✓ | ✓ | ✓ | - |
| 3.2.2.4.12 驗證申請者為網域名稱聯絡人 | ✓ | ✓ | - | - |
| 3.2.2.4.13 寄送電子郵件至 DNS CAA 聯絡人地址 | ✓ | ✓ | ✓ | - |
| 3.2.2.4.14 寄送電子郵件至 DNS TXT 聯絡人地址 | ✓ | ✓ | ✓ | - |
| 3.2.2.4.16 與 DNS TXT 紀錄電話聯絡人進行電話聯絡 | ✓ | ✓ | ✓ | - |
| 3.2.2.4.17 與 DNS CAA 電話聯絡人進行電話聯絡 | ✓ | ✓ | ✓ | - |
| 3.2.2.4.18 經約定之網站變更 v2 | - | - | - | ✓ |
| 3.2.2.4.19 經約定之網站變更 - ACME | - | - | - | ✓ |
| 3.2.2.4.20 使用 ALPN 的 TLS 連線 | - | - | - | ✓ |
| 3.2.2.4.21 標記 Account ID 之 DNS - ACME | ✓ | ✓ | - | - |
| 3.2.2.4.22 具持久性紀錄值之 DNS TXT 紀錄 | ✓ | ✓ | - | - |
| 附錄 B.2.b | ✓ | ✓ | - | ✓ |

當經授權網域名稱（ADN）為 Onion 網域名稱時，CA **應（SHALL）**依據附錄 B 進行網域驗證。

已完成之申請者授權驗證，可於一段時間內對多次憑證簽發有效。不論何種情形，該驗證流程必須在憑證核發前，於相關要求（例如本文件的第 4.2.1 節）所定之期限內發起。就網域驗證（Domain Validation）而言，「申請者」一詞包含申請者的母公司（Parent Company）、子公司（Subsidiary Company）或關係企業（Affiliate）。

由主要網路視角（Primary Network Perspective）執行之網域授權或控管權驗證相關的所有 DNS 查詢，以及 CAA 紀錄檢查，**應（MUST）**依據第 4.2.2.2 節執行 DNSSEC 驗證。

由主要網路視角執行之網域授權或控管權驗證相關的所有 DNS 查詢（包括選擇經授權網域名稱（ADN）過程中所執行之 CNAME 查詢），**應（MUST）**執行信賴鏈串鏈至 IANA DNSSEC 信賴根源（IANA DNSSEC root trust anchor）的 DNSSEC 驗證。主要網路視角用於網域授權或控管權驗證相關的所有 DNS 查詢之 DNS 解析器（DNS resolver）**應（MUST）**：

- 使用 RFC 4035 第 5 節 定義的演算法執行 DNSSEC 驗證；且

- 支援 RFC 5155 定義的 NSEC3；且
- 支援 RFC 4509 與 RFC 5702 定義的 SHA-2；且
- 妥善處理 RFC 6840 第 4 節 所列舉的安全疑慮。

對於第 3.2.2.4.4 節、第 3.2.2.4.13 節、第 3.2.2.4.14 節中描述的電子郵件（e-mail）網域驗證方法，針對由主要網路視角（Primary Network Perspective）試圖取得與網域授權或控管權驗證相關之經授權網域名稱（Authorization Domain Name）的所有 DNS CNAME、CAA、TXT 查詢，**應（MUST）**執行信賴鏈串鏈至 IANA DNSSEC 信賴根源（IANA DNSSEC root trust anchor）的 DNSSEC 驗證，且 CA **不得（MUST NOT）**利用內部政策停用 DNSSEC 驗證。對於其他所有 DNS 查詢，**宜（SHOULD）**執行信賴鏈串鏈至 IANA DNSSEC 信賴根源（IANA DNSSEC root trust anchor）的 DNSSEC 驗證，且 CA **不宜（SHOULD NOT）**利用內部政策停用 DNSSEC 驗證。

對於其他所有的網域驗證方法，由主要網路視角（Primary Network Perspective）進行之與網域授權或控管權驗證相關的所有 DNS 查詢，**應（MUST）**執行信賴鏈串鏈至 IANA DNSSEC 信賴根源（IANA DNSSEC root trust anchor）的 DNSSEC 驗證，且 CA **不得（MUST NOT）**在任何網域授權或控管權驗證相關的 DNS 查詢上利用內部政策停用 DNSSEC 驗證。

信賴鏈串鏈至 IANA DNSSEC 信賴根源的 DNSSEC 驗證，被視為不屬於為符合第 8.7 節要求而執行之內部稽核（self-audits）的範圍。

信賴鏈串鏈至 IANA DNSSEC 信賴根源的 DNSSEC 驗證，被視為不屬於第 5.4.1 節紀錄要求（logging requirements）的範圍。

**註**：FQDN 可透過 `subjectAltName` 擴充欄位中之 `dNSName` 列在用戶憑證（Subscriber Certificates）中，或透過 Name Constraints 擴充欄位中之 `permittedSubtrees` 的 `dNSName` 列在下屬憑證機構憑證（Subordinate CA Certificates）中。

#### 3.2.2.4.1 驗證申請者為網域名稱聯絡人

此方法已廢止且**不得（MUST NOT）**再使用。先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（SHALL NOT）**用於簽發憑證。

#### 3.2.2.4.2 以電子郵件、傳真、簡訊或郵寄信件至網域名稱聯絡人

此方法已廢止且**不得（MUST NOT）**再使用。先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（SHALL NOT）**用於簽發憑證。

#### 3.2.2.4.3 與網域名稱聯絡人進行電話聯絡

此方法已廢止且**不得（MUST NOT）**再使用。先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（SHALL NOT）**用於簽發憑證。

#### 3.2.2.4.4 寄送電子郵件至特定格式的地址

透過以下程序以確認申請者（Applicant）對經授權網域名稱（Authorization Domain Name，ADN）的控管權：

1. 寄送電子郵件至一個或多個郵件地址，該郵件地址以「admin」、「administrator」、「webmaster」、「hostmaster」或「postmaster」作為郵件帳號（local part），後接「@」符號，再接上經授權網域名稱（ADN）而組成；且
2. 在電子郵件中包含一組隨機值（Random Value）；且
3. 收到使用該隨機值的確認回覆。

隨機值在每封電子郵件中**應（SHALL）**是唯一的。

電子郵件**得（MAY）**全文重寄，包括重複使用隨機值，前提是其全文內容及收件者**應（SHALL）**保持不變。

隨機值自建立之日起，用於確認回覆的有效期限**應（SHALL）**不超過 30 日。憑證實務作業基準（Certification Practice Statement，CPS）**得（MAY）**規定更短的隨機值有效期限。

自 2026-03-15 起，此方法**不宜（SHOULD NOT）**用於簽發用戶憑證。

自 2028-03-15 起：

- CA **不得（MUST NOT）**依賴此方法。
- 先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（MUST NOT）**用於簽發用戶憑證。

#### 3.2.2.4.5 網域授權文件

此方法已廢止且**不得（MUST NOT）**再使用。先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（SHALL NOT）**用於簽發憑證。

#### 3.2.2.4.6 經約定之網站變更

此方法已廢止且**不得（MUST NOT）**再使用。先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（SHALL NOT）**用於簽發憑證。

#### 3.2.2.4.7 DNS 變更

藉由檢查下列任一查詢所回傳的 DNS CNAME、TXT 或 CAA 紀錄中是否存在隨機值（Random Value）或請求符記（Request Token），以確認申請者（Applicant）對經授權網域名稱（Authorization Domain Name，ADN）的控管權：

1. 經授權網域名稱（ADN）；或
2. 在經授權網域名稱（ADN）前頭加上一個以底線字元（underscore character）開頭之網域標籤（Domain Label）。

若使用隨機值，憑證機構（Certification Authority，CA）**應（SHALL）**提供該憑證申請唯一的隨機值，且在以下時間後**不得（SHALL NOT）**再使用該隨機值：

1. 30 日；或
2. 若申請者主動送出憑證申請，則期限為可重複使用與憑證相關之已驗證資料的時間允許範圍（例如本文件第 4.2.1 節或《EV 指引》第 3.2.2.14.3 節所載）。

使用此方法進行驗證的 CA **應（MUST）**實施第 3.2.2.9 節所規範之多視角簽發佐證（Multi-Perspective Issuance Corroboration）。若要算作有效佐證，其他網路視角（Network Perspective）**應（MUST）**觀察到與主要網路視角（Primary Network Perspective）相同的挑戰資訊（即隨機值或請求符記）。

若 CA 或其關係企業（Affiliate）營運一個 DNS 區域（zone），且申請者可將帶有底線開頭的網域標籤委託（透過 CNAME）至該區域，則 CA **應（MUST）**確保每位申請者委託對象的 FQDN 為該 DNS 區域內唯一的 FQDN。CA 或其關係企業**不宜（SHOULD NOT）**營運此類服務，並**宜（SHOULD）**引導使用此類服務的申請者改用第 3.2.2.4.22 節所述之方法。

#### 3.2.2.4.8 IP 位址

此方法已廢止且**不得（MUST NOT）**再使用。先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（SHALL NOT）**用於簽發憑證。

#### 3.2.2.4.9 測試憑證

此方法已廢止且**不得（MUST NOT）**再使用。先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（SHALL NOT）**用於簽發憑證。

#### 3.2.2.4.10 使用隨機值驗證 TLS 連線

此方法已廢止且**不得（MUST NOT）**再使用。先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（SHALL NOT）**用於簽發憑證。

#### 3.2.2.4.11 任何其他方法

此方法已廢止且**不得（MUST NOT）**再使用。

#### 3.2.2.4.12 驗證申請者為網域名稱聯絡人

藉由驗證申請者（Applicant）為經授權網域名稱（Authorization Domain Name，ADN）的網域名稱聯絡人（Domain Contact），以確認申請者對經授權網域名稱（ADN）的控管權。僅當經授權網域名稱（ADN）的基礎網域名稱（Base Domain Name）等於該經授權網域名稱（ADN），且憑證機構（Certification Authority，CA）同時為該經授權網域名稱（ADN）的網域名稱註冊商（Domain Name Registrar），或是該註冊商的關係企業（Affiliate）時，才得以使用此方法。

經授權網域名稱（ADN）的網域名稱聯絡人係指：登載於該經授權網域名稱（ADN）的 WHOIS 紀錄中，或透過直接聯繫網域名稱註冊商（Domain Name Registrar）所取得之註冊人（registrant）、技術聯絡人或管理聯絡人（或於國碼頂級網域名稱（ccTLD）下之同等角色）之資訊，或者該經授權網域名稱（ADN）之

SOA 紀錄中所載電子郵件地址的持有人。

簽發用戶憑證（Subscriber Certificates）時，無論先前取得之資訊是否在可重複使用的期限內，CA **不得（MUST NOT）**透過 HTTPS 網站取得網域名稱聯絡人資訊。

當 CA 為了驗證申請的網域名稱而取得網域名稱聯絡人資訊時：

- 若使用 WHOIS 協定 (RFC 3912)，**應（MUST）**查詢 IANA 的 WHOIS 伺服器，並遵從其回傳之轉介（referral）資訊，連線至適當之 WHOIS 伺服器進行查詢。
- 若使用註冊資料存取協定 (Registry Data Access Protocol，RDAP；RFC 7482)，**應（MUST）**使用 IANA 提供的 Bootstrap 檔案，以識別並查詢該網域所對應之正確的 RDAP 伺服器。
- **不得（MUST NOT）**依賴超過 48 小時之（1）WHOIS 伺服器快取資訊，或（2）IANA 提供的 RDAP Bootstrap 資料快取，以確保其依賴最新且正確的資訊。

### 3.2.2.4.13 寄送電子郵件至 DNS CAA 聯絡人地址

藉由透過電子郵件寄送隨機值（Random Value），並接收使用該隨機值的確認回覆，以確認申請者（Applicant）對經授權網域名稱（Authorization Domain Name，ADN）的控管權。隨機值**應（MUST）**寄送至 DNS CAA 電子郵件聯絡人（DNS CAA Email Contact）的地址。相關的 CAA 資源紀錄集（Resource Record Set）**應（MUST）**使用 RFC 8659 第 3 節 定義的搜尋演算法尋找。

每一封電子郵件**得（MAY）**確認多個經授權網域名稱（ADN）的控管權，前提是每個電子郵件地址皆為每一個待驗證之經授權網域名稱（ADN）的 DNS CAA 電子郵件聯絡人的地址。同一封電子郵件**得（MAY）**寄送至多個收件者，前提是每個電子郵件地址皆為每一個待驗證之經授權網域名稱（ADN）的 DNS CAA 電子郵件聯絡人的地址。

隨機值在每封電子郵件中**應（SHALL）**是唯一的。電子郵件**得（MAY）**全文重寄，包括重複使用隨機值，前提是其全文內容及收件者**應（SHALL）**保持不變。隨機值自建立之日起，用於確認回覆的有效期限**應（SHALL）**不超過 30 日。憑證實務作業基準（Certification Practice Statement，CPS）**得（MAY）**規定更短的隨機值有效期限。

使用此方法進行驗證的 CA **應（MUST）**實施第 3.2.2.9 節所規範之多視角簽發佐證（Multi-Perspective Issuance Corroboration）。若要算作有效佐證，其他網路視角（Network Perspective）**應（MUST）**觀察到與主要網路視角（Primary Network Perspective）相同的網域驗證之聯絡人資訊。

自 2026-03-15 起，此方法**不宜（SHOULD NOT）**用於簽發用戶憑證。

自 2028-03-15 起：

- CA **不得（MUST NOT）**依賴此方法。
- 先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（MUST NOT）**用於簽發用戶憑證。

### 3.2.2.4.14 寄送電子郵件至 DNS TXT 聯絡人地址

藉由透過電子郵件寄送隨機值（Random Value），並接收使用該隨機值的確認回覆，以確認申請者（Applicant）對經授權網域名稱（Authorization Domain Name，ADN）的控管權。隨機值**應（MUST）**寄送至該經授權網域名稱（ADN）的 DNS TXT 紀錄電子郵件聯絡人（DNS TXT Record Email Contact）的地址。

每一封電子郵件**得（MAY）**確認多個經授權網域名稱（ADN）的控管權，前提是每個電子郵件地址皆為每一個待驗證之經授權網域名稱（ADN）的 DNS TXT 紀錄電子郵件聯絡人的地址。同一封電子郵件**得（MAY）**寄送至多個收件者，前提是每個電子郵件地址皆為每一個待驗證之經授權網域名稱（ADN）的 DNS TXT 紀錄電子郵件聯絡人的地址。

隨機值在每封電子郵件中**應（SHALL）**是唯一的。電子郵件**得（MAY）**全文重寄，包括重複使用隨機值，前提是其全文內容及收件者**應（SHALL）**保持不變。隨機值自建立之日起，用於確認回覆的有效期限**應（SHALL）**不超過 30 日。憑證實務作業基準（Certification Practice Statement，CPS）**得（MAY）**規定更短的隨機值有效期限。

使用此方法進行驗證的 CA **應（MUST）**實施第 3.2.2.9 節所規範之多視角簽發佐證（Multi-Perspective Issuance Corroboration）。若要算作有效佐證，其他網路視角（Network Perspective）**應（MUST）**觀察到與主要網路視角（Primary Network Perspective）相同的網域驗證之聯絡人資訊。

自 2026-03-15 起，此方法**不宜（SHOULD NOT）**用於簽發用戶憑證。

自 2028-03-15 起：

- CA **不得（MUST NOT）**依賴此方法。
- 先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（MUST NOT）**用於簽發用戶憑證。

### 3.2.2.4.15 與網域名稱聯絡人進行電話聯絡

此方法已廢止且**不得（MUST NOT）**再使用。先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（SHALL NOT）**用於簽發憑證。

### 3.2.2.4.16 與 DNS TXT 紀錄電話聯絡人進行電話聯絡

藉由撥打 DNS TXT 紀錄電話聯絡人（DNS TXT Record Phone Contact）的電話號碼並取得確認回覆，以確認申請者（Applicant）對經授權網域名稱（Authorization Domain Name，ADN）的控管權。每次通話**得（MAY）**確認多個經授權網域名稱（ADN）的控管權，前提是每一個待驗證之經授權網域名稱（ADN）均列出相同的 DNS TXT 紀錄電話聯絡人的號碼，且接聽者對每一個經授權網域名稱（ADN）分別做出確認回覆。

憑證機構（Certification Authority，CA）**不得（MUST NOT）**在明知電話被轉接的情況下繼續驗證，或要求轉接至其他對象，因為該電話號碼是專門為網域驗證（Domain Validation）而列在 DNS TXT 紀錄中。

若進入語音信箱，CA 得留下隨機值（Random Value）及正在驗證的經授權網域名稱（ADN）。隨機值**應（MUST）**被回傳給 CA 以核准驗證請求。

隨機值自建立之日起，用於確認回覆的有效期限**應（SHALL）**不超過 30 日。憑證實務作業基準（Certification Practice Statement，CPS）**得（MAY）**規定更短的隨機值有效期限。

使用此方法進行驗證的 CA **應（MUST）**實施第 3.2.2.9 節所規範之多視角簽發佐證（Multi-Perspective Issuance Corroboration）。若要算作有效佐證，其他網路視角（Network Perspective）**應（MUST）**觀察到與主要網路視角（Primary Network Perspective）相同的網域驗證之聯絡人資訊。

自 2026-03-15 起，此方法**不宜（SHOULD NOT）**用於簽發用戶憑證。

自 2027-03-15 起：

- CA **不得（MUST NOT）**依賴此方法。
- 先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（MUST NOT）**用於簽發用戶憑證。

### 3.2.2.4.17 與 DNS CAA 電話聯絡人進行電話聯絡

藉由撥打 DNS CAA 電話聯絡人（DNS CAA Phone Contact）的電話號碼，並取得確認回覆以驗證該經授權網域名稱（Authorization Domain Name，ADN），以確認申請者（Applicant）對經授權網域名稱（ADN）的控管權。每次通話**得（MAY）**確認多個經授權網域名稱（ADN）的控管權，前提是每一個待驗證之經授權網域名稱（ADN）均列出相同的 DNS CAA 電話聯絡人的號碼，且接聽者對每一個經授權網域名稱（ADN）分別做出確認回覆。相關的 CAA 資源紀錄集（Resource Record Set）**應（MUST）**使用 RFC 8659 第 3 節 定義的搜尋演算法尋找。

憑證機構（Certification Authority，CA）**不得（MUST NOT）**接受電話被轉接，或要求轉接至其他對象，因為該電話號碼是專門為網域驗證（Domain Validation）而列出。

若進入語音信箱，CA 得留下隨機值（Random Value）及正在驗證的經授權網域名稱（ADN）。隨機值**應（MUST）**被回傳給 CA 以核准驗證請求。

隨機值自建立之日起，用於確認回覆的有效期限**應（SHALL）**不超過 30 日。憑證實務作業基準（Certification Practice Statement，CPS）**得（MAY）**規定更短的隨機值有效期限。

使用此方法進行驗證的 CA **應（MUST）**實施第 3.2.2.9 節所規範之多視角簽發佐證（Multi-Perspective Issuance Corroboration）。若要算作有效佐證，其他網路視角（Network Perspective）**應（MUST）**觀察到與主要網路視角（Primary Network Perspective）相同的網域驗證之聯絡人資訊。

自 2026-03-15 起，此方法**不宜（SHOULD NOT）**用於簽發用戶憑證。

自 2027-03-15 起：

- CA **不得（MUST NOT）**依賴此方法。

- 先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（MUST NOT）**用於簽發用戶憑證。

### 3.2.2.4.18 經約定之網站變更 v2

透過驗證特定檔案內容中所包含的請求符記（Request Token）或隨機值（Random Value），以確認申請者（Applicant）對經授權網域名稱（Authorization Domain Name，ADN）的控管權。

1. 完整的請求符記或隨機值**不得（MUST NOT）**出現於用來獲取該檔案的請求路徑中，且
2. CA **應（MUST）**從該請求收到成功的 HTTP 回應（意即必須收到 2xx HTTP 狀態碼）。

內容包含請求符記或隨機值的特定檔案：

1. **應（MUST）**位於該經授權網域名稱（ADN）之網址，且
2. **應（MUST）**位於 “/.well-known/pki-validation” 目錄下，且
3. **應（MUST）**透過 “http” 或 “https” 協定獲取，且
4. **應（MUST）**透過授權連接埠（Authorized Port）存取。

若 CA 接受並遵從重新導向（redirects），則必須符合以下規定：

1. 重新導向**應（MUST）**於 HTTP 協定層發起。重新導向**應（MUST）**由狀態碼為 RFC 7231 第 6.4 節 所定義之 301、302 或 307，或 RFC 7538 第 3 節 所定義之 308 的 HTTP 回應所觸發。重新導向的目標**應（MUST）**為 RFC 7231 第 7.1.2 節 所定義之 HTTP 回應標頭 Location 的最終值。
2. 重新導向**應（MUST）**導向具有 “http” 或 “https” 協定的資源 URL 網址。
3. 重新導向**應（MUST）**導向經由授權連接埠（Authorized Ports）存取的資源 URL 網址。

若使用隨機值（Random Value），則：

1. CA **應（MUST）**針對該憑證申請提供唯一的隨機值。
2. 隨機值自建立之日起，用於確認回覆的有效期限**應（MUST）**不超過 30 日。憑證實務作業基準（Certification Practice Statement，CPS）**得（MAY）**規定更短的隨機值有效期限，在此情況下，CA **應（MUST）**遵從其憑證實務作業基準（CPS）。

除 Onion 網域名稱（Onion Domain Names）外，使用此方法進行驗證的 CA **應（MUST）**實施第 3.2.2.9 節所規範之多視角簽發佐證（Multi-Perspective Issuance Corroboration）。若要算作有效佐證，其他網路視角（Network Perspective）**應（MUST）**觀察到與主要網路視角（Primary Network Perspective）相同的挑戰資訊（即隨機值或請求符記）。

### 3.2.2.4.19 經約定之網站變更 - ACME

透過使用 RFC 8555 第 8.3 節 所定義的 ACME HTTP 挑戰（Challenge）方法，以確認申請者（Applicant）對經授權網域名稱（Authorization Domain Name，ADN）的控管權。除 RFC 8555 所規定之要求外，尚應符合下列額外要求。

憑證機構（Certification Authority，CA）**應（MUST）**從該請求收到成功的 HTTP 回應（意即必須收到 2xx HTTP 狀態碼）。

Token（如 RFC 8555 第 8.3 節 所定義）自建立之日起，**不得（MUST NOT）**使用超過 30 日。憑證實務作業基準（Certification Practice Statement，CPS）**得（MAY）**規定更短的隨機值有效期限，在此情況下，CA **應（MUST）**遵從其憑證實務作業基準（CPS）。

若 CA 接受並遵從重新導向（redirects），則必須符合以下規定：

1. 重新導向**應（MUST）**於 HTTP 協定層發起。重新導向**應（MUST）**由狀態碼為 RFC 7231 第 6.4 節 所定義之 301、302 或 307，或 RFC 7538 第 3 節 所定義之 308 的 HTTP 回應所觸發。重新導向的目標**應（MUST）**為 RFC 7231 第 7.1.2 節 所定義之 HTTP 回應標頭 Location 的最終值。
2. 重新導向**應（MUST）**導向具有 “http” 或 “https” 協定的資源 URL 網址。
3. 重新導向**應（MUST）**導向經由授權連接埠（Authorized Ports）存取的資源 URL 網址。

除 Onion 網域名稱（Onion Domain Names）外，使用此方法進行驗證的 CA **應（MUST）**實施第 3.2.2.9 節所規範之多視角簽發佐證（Multi-Perspective Issuance Corroboration）。若要算作有效佐證，其他網路視角（Network Perspective）**應（MUST）**觀察到與主要網路視角（Primary Network Perspective）相同的挑戰資訊（即 ACME 使用的 Token）。

### 3.2.2.4.20 使用 ALPN 的 TLS 連線

透過使用 RFC 7301 定義的 TLS Application-Layer Protocol Negotiation（ALPN）擴充功能（Extension），並依 RFC 8737 所定義之程序協商一個新的應用層協定，以確認申請者（Applicant）對經授權網域名稱（Authorization Domain Name，ADN）的控管權。除 RFC 8737 所規定之要求外，尚應符合下列額外要求。

Token（如 RFC 8737 第 3 節 所定義）自建立之日起，**不得（MUST NOT）**使用超過 30 日。憑證實務作業基準（Certification Practice Statement，CPS）**得（MAY）**規定更短的隨機值有效期限，在此情況下，CA **應（MUST）**遵從其憑證實務作業基準（CPS）。

除 Onion 網域名稱（Onion Domain Names）外，使用此方法進行驗證的 CA **應（MUST）**實施第 3.2.2.9 節所規範之多視角簽發佐證（Multi-Perspective Issuance Corroboration）。若要算作有效佐證，其他網路視角（Network Perspective）**應（MUST）**觀察到與主要網路視角（Primary Network Perspective）相同的挑戰資訊（即 ACME 使用的 Token）。

### 3.2.2.4.21 標記 Account ID 之 DNS - ACME

透過執行 https://datatracker.ietf.org/doc/draft-ietf-acme-dns-account-label/ 所記載之《Automated Certificate Management Environment (ACME) DNS Labeled With ACME Account ID Challenge》第 00 版草案（draft 00）中針對「dns-account-01」挑戰所規定之程序，以確認申請者（Applicant）對經授權網域名稱（Authorization Domain Name，ADN）的控管權。

Token（定義於《Automated Certificate Management Environment (ACME) DNS Labeled With ACME Account ID Challenge》第 00 版草案第 3.1 節）自建立之日起，**不得（MUST NOT）**使用超過 30 日。憑證實務作業基準（Certification Practice Statement，CPS）**得（MAY）**規定更短的隨機值有效期限，在此情況下，CA **應（MUST）**遵從其憑證實務作業基準（CPS）。

使用此方法進行驗證的 CA **應（MUST）**實施第 3.2.2.9 節所規範之多視角簽發佐證（Multi-Perspective Issuance Corroboration）。若要算作有效佐證，其他網路視角（Network Perspective）**應（MUST）**觀察到與主要網路視角（Primary Network Perspective）相同的 Token。

### 3.2.2.4.22 具持久性紀錄值之 DNS TXT 紀錄

透過檢查持久性 DCV TXT 紀錄（Persistent DCV TXT Record）是否存在來識別申請者（Applicant）身分，以確認申請者對經授權網域名稱（Authorization Domain Name，ADN）的控管權。該紀錄**應（MUST）**設置於待驗證之經授權網域名稱（ADN）加上前頭的「`_validation-persist`」標籤所形成的 DNS 紀錄名稱（即「`_validation-persist.[經授權網域名稱]`」）下。

憑證機構（Certification Authority，CA）**應（MUST）**確認持久性 DCV TXT 紀錄的 RDATA 值符合以下要求：

1. RDATA 值**應（MUST）**符合 RFC 8659 第 4.2 節 所定義的 `issue-value` 語法；且
2. `issuer-domain-name` 之值**應（MUST）**為 CA 於憑證政策（Certificate Policy，CP）及／或憑證實務作業基準（Certification Practice Statement，CPS）第 4.2 節中記載的簽發者網域名稱（Issuer Domain Name）；且
3. `issue-value` **應（MUST）**包含 `accounturi` 參數，其參數值為唯一 URI（如 RFC 8657 第 3 節 所述），用以識別請求 FQDN 驗證的申請者帳號；且
4. `issue-value` **得（MAY）**包含 `persistUntil` 參數。若該參數存在，其參數值**應（MUST）**為 10 進位編碼的整數，代表 UNIX 時間戳記（自 1970-01-01T00:00:00Z 起計算的秒數，忽略閏秒）；且
5. `issue-value` **得（MAY）**包含額外的參數。CA **應（MUST）**忽略任何未知的參數名稱（Parameter Key）。

若存在 `persistUntil` 參數，CA **應（MUST）**評估其參數值。若檢查的時間晚於 `persistUntil` 參數值所指定的時間，CA **不得（MUST NOT）**將該紀錄作為申請者擁有 FQDN 控管權之證據。

例如，持久性 DCV TXT 紀錄看起來可能像：`_validation-persist.example.com IN TXT "authority.example; accounturi=https://authority.example/acct/123; persistUntil=1782424856"`

為了符合第 4.2.1 節之方針，對於使用此方法完成之驗證，CA **應（MUST）**將 10 日視為可重複使用已驗證資料之最大天數。

下表顯示 `persistUntil` 參數在不同的時間點，如何影響 DNS 紀錄是否可被用於驗證：

| 驗證之日期／時間 | persistUntil | 是否可用於驗證 | 說明 |
| --- | --- | --- | --- |
| 2025-06-15T12:00:00Z | 2026-01-01T00:00:00Z (1767225600) | 是 | 驗證時間早於 persistUntil 時間戳記，因此該紀錄可用 |
| 2025-06-15T12:00:00Z | 2025-01-01T00:00:00Z (1735689600) | 否 | 驗證時間晚於 persistUntil 時間戳記，因此該紀錄不可用 |
| 2025-06-15T12:00:00Z | (未提供) | 是 | 未提供 persistUntil 參數，因此不適用時間限制 |

`persistUntil` 參數如何影響驗證之範例

使用此方法進行驗證的 CA **應（MUST）**實施第 3.2.2.9 節所規範之多視角簽發佐證（Multi-Perspective Issuance Corroboration）。若要算作有效佐證，其他網路視角（Network Perspective）**應（MUST）**觀察到申請者證明其網域控管權的持久性 DCV TXT 紀錄，且其中包含與主要網路視角（Primary Network Perspective）相同的 `accounturi` 參數。

### 3.2.2.5 IP 位址之鑑別

本節定義憑證機構（Certification Authority，CA）驗證申請者（Applicant）對憑證中所列 IP 位址（IP Address）的所有權或控管權之允許流程與程序。

CA **應（SHALL）**於簽發前確認，CA 至少已使用本節指定的一種方法驗證憑證中所列 IP 位址。

已完成的申請者授權驗證，可於一段時間內對多次憑證簽發有效。不論何種情形，該驗證流程必須在憑證核發前，於相關要求（例如本文件的第 4.2.1 節）所定之期限內發起。就 IP 位址驗證（IP Address validation）而言，「申請者」一詞包含申請者的母公司（Parent Company）、子公司（Subsidiary Company）或關係企業（Affiliate）。

#### 3.2.2.5.1 經約定之網站變更

確認憑證機構（Certification Authority，CA）可透過 HTTP/HTTPS 在授權連接埠（Authorized Port）存取 IP 位址（IP Address）上的特定檔案或網頁，檢查內容是否存在以 HTML <meta> 標籤包含的請求符記（Request Token）或隨機值（Random Value），以確認申請者（Applicant）對所請求 IP 位址的控管權。該檔案或網頁必須位於「/.well-known/pki-validation」目錄下，或者用以驗證 IP 位址控管權而由 IANA 登記的其他路徑。請求符記或隨機值**不得（MUST NOT）**出現在請求 IP 的驗證路徑中。

若使用隨機值，CA **應（SHALL）**提供該憑證申請唯一的隨機值，且在以下最長期限後**不得（SHALL NOT）**再使用該隨機值：

i. 30 日；或

ii. 若申請者主動送出憑證申請，則期限為可重複使用與憑證相關之已驗證資料的時間允許範圍（例如本文件第 4.2.1 節所載）。

使用此方法進行驗證的 CA **應（MUST）**實施第 3.2.2.9 節所規範之多視角簽發佐證（Multi-Perspective Issuance Corroboration）。若要算作有效佐證，其他網路視角（Network Perspective）**應（MUST）**觀察到與主要網路視角（Primary Network Perspective）相同的挑戰資訊（即隨機值或請求符記）。

#### 3.2.2.5.2 以電子郵件、傳真、簡訊或郵寄信件至 IP 位址聯絡人

藉由透過電子郵件、傳真、簡訊或郵寄信件發送隨機值（Random Value），並接收使用該隨機值的確認回覆，以確認申請者（Applicant）對 IP 位址（IP Address）的控管權。隨機值**應（MUST）**發送至被識別為 IP 位址聯絡人（IP Address Contact）的電子郵件位址、傳真／簡訊號碼或郵寄信件地址。

每封電子郵件、傳真、簡訊或郵寄信件**得（MAY）**確認多個 IP 位址的控管權。

憑證機構（Certification Authority，CA）**得（MAY）**將本節所規定的電子郵件、傳真、簡訊或郵寄信件發送予多位收件者，前提是 IP 位址註冊管理機構（IP Address Registration Authority）將每位收件者識別為每個待驗證 IP 位址的聯絡人，該驗證使用電子郵件、傳真、簡訊或郵寄信件進行。

隨機值在每封電子郵件、傳真、簡訊或郵寄信件中**應（SHALL）**是唯一的。

CA **得（MAY）**全文重送電子郵件、傳真、簡訊或郵寄信件，包括重複使用隨機值，前提是該通訊的全文內容及收件者保持不變。

隨機值自建立之日起，用於確認回覆的有效期限**應（SHALL）**不超過 30 日。憑證實務作業基準（Certification Practice Statement，CPS）**得（MAY）**規定更短的隨機值有效期限，在此情況下，CA **應（MUST）**遵從其憑證實務作業基準（CPS）。

自 2026-03-15 起，此方法**不宜（SHOULD NOT）**用於簽發用戶憑證。

自 2027-03-15 起：

- CA **不得（MUST NOT）**依賴此方法。
- 先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（MUST NOT）**用於簽發用戶憑證。

#### 3.2.2.5.3 反向位址查詢

藉由對 IP 位址（IP Address）進行反向 IP 查詢以取得與該 IP 位址關聯的完全吻合網域名稱（Fully-Qualified Domain Name，FQDN），再將該 FQDN 作為經授權網域名稱（Authorization Domain Name，ADN），並使用第 3.2.2.4 節允許的方法進行驗證，以確認申請者（Applicant）對該 IP 位址的控管權。自 2026-11-15 起，此方法所使用的經授權網域名稱（ADN）**應（MUST）**與反向 IP 查詢所回傳的 FQDN 完全相同；第 3.2.2.4 節所述的選擇經授權網域名稱（ADN）的判斷流程不適用。

使用此方法進行驗證的憑證機構（Certification Authority，CA）**應（MUST）**實施第 3.2.2.9 節所規範之多視角簽發佐證（Multi-Perspective Issuance Corroboration）。若要算作有效佐證，其他網路視角（Network Perspective）**應（MUST）**觀察到與主要網路視角（Primary Network Perspective）相同的 FQDN。

自 2027-03-15 起：

- CA **不得（MUST NOT）**依賴此方法。
- 先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（MUST NOT）**用於簽發用戶憑證。

#### 3.2.2.5.4 任何其他方法

此方法已廢止且**不得（MUST NOT）**再使用。先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（SHALL NOT）**用於簽發憑證。

#### 3.2.2.5.5 與 IP 位址聯絡人進行電話聯絡

藉由撥打 IP 位址聯絡人（IP Address Contact）的電話號碼，並取得申請者（Applicant）請求 IP 位址（IP Address）驗證的確認回覆，以確認申請者對 IP 位址的控管權。憑證機構（Certification Authority，CA）**應（MUST）**將電話撥打至由 IP 位址註冊管理機構（IP Address Registration Authority）識別為 IP 位址聯絡人的電話號碼。每通電話**應（SHALL）**只撥打至單一號碼。

如果接通了 IP 位址聯絡人以外的人員，憑證機構**得（MAY）**要求轉接給 IP 位址聯絡人。

若進入語音信箱，CA 得留下隨機值（Random Value）和正在驗證的 IP 位址。隨機值**應（MUST）**被回傳給 CA 以核准驗證請求。

隨機值自建立之日起，用於確認回覆的有效期限**應（SHALL）**不超過 30 日。憑證實務作業基準（Certification Practice Statement，CPS）**得（MAY）**規定更短的隨機值有效期限。

自 2026-03-15 起，此方法**不宜（SHOULD NOT）**用於簽發用戶憑證。

自 2027-03-15 起：

- CA **不得（MUST NOT）**依賴此方法。
- 先前使用此方法進行的驗證，以及依據此方法蒐集的驗證資料，**不得（MUST NOT）**用於簽發用戶憑證。

#### 3.2.2.5.6 IP 位址之 ACME http-01 方法

透過執行 RFC 8738 中針對「http-01」挑戰所規定之程序，以確認申請者（Applicant）對 IP 位址（IP Address）的控管權。

使用此方法進行驗證的 CA **應（MUST）**實施第 3.2.2.9 節所規範之多視角簽發佐證（Multi-Perspective Issuance Corroboration）。若要算作有效佐證，其他網路視角（Network Perspective）**應（MUST）**觀察到與主要網路視角（Primary Network Perspective）相同的挑戰資訊（即 ACME 使用的 Token）。

#### 3.2.2.5.7 IP 位址之 ACME tls-alpn-01 方法

透過執行 RFC 8738 中針對「tls-alpn-01」挑戰所規定之程序，以確認申請者（Applicant）對 IP 位址（IP Address）的控管權。

使用此方法進行驗證的 CA **應（MUST）**實施第 3.2.2.9 節所規範之多視角簽發佐證（Multi-Perspective Issuance Corroboration）。若要算作有效佐證，其他網路視角（Network Perspective）**應（MUST）**觀察到與主要網路視角（Primary Network Perspective）相同的挑戰資訊（即 ACME 使用的 Token）。

#### 3.2.2.5.8 反向名稱空間中具持久性紀錄值之 DNS TXT 紀錄

透過將 IP 位址（IP Address）轉換為反向區域網域名稱（Reverse Zone Domain Name），隨後依第 3.2.2.4.22 節所定義的持久性 DCV TXT 紀錄是否存在來識別申請者（Applicant）身分，以確認申請者對 IP 位址的控管權。該紀錄**應（MUST）**設置於待驗證之 IP 位址反向區域網域名稱加上前頭的「`_ip-validation-persist`」標籤所形成的 DNS 紀錄名稱（即「`_ip-validation-persist.[反向區域網域名稱]`」）下。

### 3.2.2.6 萬用網域名稱之驗證

於簽發萬用網域憑證（Wildcard Certificate）之前，憑證機構（Certification Authority，CA）**應（MUST）**建立並遵從一套書面程序，以判斷憑證中任何萬用網域名稱（Wildcard Domain Name）之完全吻合網域名稱（Fully-Qualified Domain Name，FQDN）字串是否屬於「註冊表控制網域（registry-controlled）」或「公開字尾（public suffix）」（例如：“*.com”、“*.co.uk”，進一步說明請參見 RFC 6454 第 8.2 節）。

若任何萬用網域名稱之 FQDN 字串屬於「註冊表控制網域」或「公開字尾」，CA **應（MUST）**拒絕簽發，除非申請者（Applicant）證明其對整個網域名稱空間具有合法控管權。（例如：CA **不得（MUST NOT）**簽發 “*.co.uk” 或 “*.local”，但**得（MAY）**簽發 “*.example.com” 給 Example Co.）。

在撰寫本文時，對於國碼頂級網域名稱空間（ccTLD Namespace）中，如何區分「註冊表控制網域」與可註冊字串（registerable portion）的判斷規則，尚未標準化，且此資訊並非 DNS 本身所提供的屬性。當前最佳實務做法是參考「公開字尾清單」——公開字尾清單（Public Suffix List，PSL），並定期取得最新內容。

若要使用 PSL，CA **宜（SHOULD）**僅查閱「ICANN DOMAINS」部分，而不查閱「PRIVATE DOMAINS」部分。PSL 會定期更新以收錄由 ICANN 委派的新通用頂級網域名稱（generic Top-Level Domains，gTLDs），這些網域名稱被列在「ICANN DOMAINS」部分內。CA 並不被禁止簽發萬用網域憑證給整個 gTLD 的註冊人（Registrant），前提是要以適當的方式證明其對整個名稱空間（namespace）的控管權。

### 3.2.2.7 資料來源的正確性

於使用任何資料來源作為可靠資料來源（Reliable Data Source）之前，憑證機構（Certification Authority，CA）**應（SHALL）**評估此來源的可靠性、準確性，以及防竄改或防偽造的能力。CA 在評估過程**宜（SHOULD）**考慮以下事項：

1. 所提供資訊的時效性，

2. 資訊來源的更新頻率，

3. 資料提供者和資料收集之目的，

4. 大眾取得可用資料的便利性，以及

5. 偽造或竄改資料的相對難度。

由 CA、其擁有者或其關係企業（Affiliate）所維護之資料庫，若該資料庫之主要目的是為了蒐集資訊以符合本文件第 3.2 節的驗證要求，則不符合可靠資料來源的資格。

#### 3.2.2.8 授權憑證機構簽發憑證（CAA）紀錄

CAA 紀錄處理之要求，請參見第 4.2.2.1 節。

#### 3.2.2.8.1 授權憑證機構簽發憑證（CAA）紀錄的 DNSSEC 驗證

CAA 紀錄處理之 DNSSEC 驗證要求，請參見第 4.2.2.2 節。

#### 3.2.2.9 多視角簽發佐證（Multi-Perspective Issuance Corroboration）

多視角簽發佐證（Multi-Perspective Issuance Corroboration）試圖在憑證簽發之前，從多個遠端網路視角（Remote Network Perspectives）佐證由主要網路視角（Primary Network Perspective）所做出的判定結果（即網域驗證通過／失敗、CAA 許可／禁止）。此流程可提升相同路由前綴長度（equally-specific prefix）之邊界閘道協定（Border Gateway Protocol，BGP）攻擊或劫持的防護能力。

當針對所需之（1）網域授權或控管權驗證，及（2）CAA 紀錄檢查而執行多視角簽發佐證時，憑證機構（Certification Authority，CA）**得（MAY）**兩者都使用相同組合或不同組合之網路視角。

作為判定依據的網路視角回應集合**應（MUST）**向 CA 提供必要資訊，以允許其明確評估：

a. 是否存在預期之（1）隨機值（Random Value）、（2）請求符記（Request Token）、（3）IP 位址（IP Address）、（4）聯絡地址，或（5）持久性 DCV TXT 紀錄，如同採用第 3.2.2.4 節及第 3.2.2.5 節所列驗證方法之規定要求；以及

b. CA 是否可依第 4.2.2.1 節規定獲得授權，對申請中的網域簽發憑證。

第 3.2.2.4 節與第 3.2.2.5 節說明哪些網域驗證方法須採用多視角簽發佐證，以及其他網路視角如何佐證由主要網路視角所做出的判定結果。

當接續使用其他網路視角進行驗證時，**不得（MUST NOT）**重複使用或快取（cache）任一網路視角所取得之結果或資訊（例如：不同的網路視角不得依賴共用的 DNS 快取，以避免控制其中一個網路視角流量之攻擊者，污染其他網路視角所使用的 DNS 快取）。為網路視角提供網際網路連線的網路基礎設施，**得（MAY）**由提供該網路視角運作所需運算服務之同一組織管理。遠端網路視角與 CA 之間的所有通訊**應（MUST）**透過採用現代協定（例如：透過 HTTPS）的經身分驗證且加密之通道進行。

網路視角**得（MAY）**使用未與該網路視角同地設置的遞迴 DNS 解析器。然而，該網路視角所使用的 DNS 解析器**應（MUST）**與使用該解析器的網路視角位於同一個區域網際網路註冊管理機構（Regional Internet Registry）的服務區域內。此外，在一次多視角簽發佐證執行中所使用的 DNS 解析器，任兩個 DNS 解析器之間的直線距離**應（MUST）**至少為 500 公里。DNS 解析器的位置，通常係指未封裝之對外 DNS 查詢首次交接給提供該 DNS 解析器網際網路連線之網路基礎設施的地點。

CA **得（MAY）**立即使用相同的驗證方法或替代驗證方法重新執行多視角簽發佐證（例如：若「經約定之網站變更 - ACME」的多視角簽發佐證結果無法成立，CA 可立即使用「寄送電子郵件至 DNS TXT 聯絡人地址」重新執行驗證）。當重新執行多視角簽發佐證時，CA **不得（MUST NOT）**依據先前取得之佐證資訊。對於任何期間內可執行的驗證次數上限，本文件不作規定。

「法定數量要求（Quorum Requirements）」表格列出多視角簽發佐證的法定數量（Quorum）要求。若 CA 在進行網域授權或控管權驗證與 CAA 紀錄檢查時，兩者均**未**採用相同組合之網路視角，則兩組網路視角（即網域授權或控管權驗證組與 CAA 紀錄檢查組）**應（MUST）**皆符合法定數量要求。當網路視角彼此間的直線距離至少為 500 公里時，被視為彼此相異（distinct）。當某一網路視角與主要網路視角，以及法定數量中的其他網路視角皆為相異時，該網路視角即視為「遠端」。

CA **得（MAY）**重複使用 CAA 紀錄檢查符合法定數量要求的佐證證明，最長不超過 398 日。向某網域簽發憑證後，針對同一申請者之後續憑證申請，遠端網路視角**得（MAY）**省略取得及處理相同網域或其子網域的 CAA 紀錄，最長不超過 398 日。

| 相異的遠端網路視角數量 | 容許無效佐證的遠端網路視角數量 |
| --- | --- |
| 2-5 | 1 |
| 6+ | 2 |

法定數量要求表

執行多視角簽發佐證的遠端網路視角：

**應（MUST）：**

- 網路強化（Network Hardening）
  - 依賴已採取對應措施，可於全球網際網路路由系統中，降低受 BGP 路由事故影響之網路供應服務（例如：網際網路服務供應商或雲端服務供應商的網路），對該網路視角提供網際網路連線。

**宜（SHOULD）：**

- 設施與服務供應商要求
  - 託管於通過 ISO/IEC 27001 認證的設施，或經獨立稽核且通過認證或出具稽核報告之同等安全架構的設施。

    - 依賴受下列任一稽核報告查核涵蓋之供應服務：System and Organization Controls 2（SOC 2）、ISAE 3000、ENISA 715、FedRAMP Moderate、C5:2020、CSA STAR CCM，或其他經獨立稽核且通過認證或出具稽核報告之同等服務架構。
- 弱點偵測與修補程式管理
    - 實施入侵偵測與入侵防護控管措施，以防範常見的網路及系統威脅。
    - 建立書面文件化的弱點修正流程並據以執行，該流程應涵蓋弱點之識別、審查、回應及修補。
    - 至少每 3 個月接受或執行一次弱點掃描。
    - 至少每年接受一次滲透測試。
    - 於安全修補程式可取得後 6 個月內套用建議的安全修補程式，除非 CA 以書面文件記錄並說明，該安全修補程式會引入額外的弱點或不穩定性，且其風險大於套用該安全修補程式所帶來的效益。
- 系統強化（System Hardening）
    - 停用所有未使用的帳號、應用程式、服務、通訊協定及連接埠。
    - 對所有使用者帳號實施多因子身分驗證。
- 網路強化
    - 對每個網路邊界控制（防火牆、交換器、路由器、閘道器或其他網路控制設備或系統）配置規則，使其僅允許經識別為其運作所需之服務、通訊協定、連接埠和通訊之流量通過。
    - 依賴符合下列條件之網路供應服務（例如：網際網路服務供應商）：（1）採用基於 Secure Inter-Domain Routing（SIDR，安全網域間路由；RFC 6480）安全架構的機制，例如 BGP 路由前綴來源驗證（BGP Prefix Origin Validation；RFC 6811），（2）採用其他非 RPKI 的路由洩漏防範機制（例如 RFC 9234），以及（3）導入 BCP 194 所述的當前最佳實務。此外，雖然**建議（RECOMMENDED）**在正常運作情況下，執行多視角簽發佐證的網路視角應透過一個或多個依 RFC 6811 規範，過濾經 RPKI 驗證為無效之 BGP 路由的網路來轉送所有網際網路流量，但這屬於**非強制要求（NOT REQUIRED）**。

除以上要求外，執行多視角簽發佐證的運算系統，被視為不屬於本文件第 8 節所述之稽核範圍。

若上述任何要求（considerations）是由受委任第三方（Delegated Third Party）執行，CA **得（MAY）**自受委任第三方取得合理證明，以查明並確信上述一項或多項要求已獲得遵從。作為第 1.3.2 節之例外，受委任第三方無須為了符合上述各項要求，而納入本文件第 8 節所述之稽核範圍。

分階段實施時程：

- 自 2025-03-15 起：CA **應（MUST）**使用至少 2 個遠端網路視角進行多視角簽發佐證。若無法佐證主要網路視角所做判定的遠端網路視角數量（「無效佐證」）大於《法定數量要求表》所允許的數量，CA **得（MAY）**繼續進行憑證簽發。

- 自 2025-09-15 起：CA **應（MUST）**使用至少 2 個遠端網路視角進行多視角簽發佐證。CA **應（MUST）**確保符合《法定數量要求表》所定義的要求。若未符合該等要求，則 CA **不得（MUST NOT）**繼續簽發憑證。
- 自 2026-03-15 起：CA **應（MUST）**使用至少 3 個遠端網路視角進行多視角簽發佐證。CA **應（MUST）**確保符合《法定數量要求表》所定義的要求，且佐證主要網路視角的遠端網路視角分別位於至少 2 個不同的區域網際網路註冊管理機構（Regional Internet Registries）服務區域內。若未符合該等要求，則 CA **不得（MUST NOT）**繼續簽發憑證。
- 自 2026-06-15 起：CA **應（MUST）**使用至少 4 個遠端網路視角進行多視角簽發佐證。CA **應（MUST）**確保符合《法定數量要求表》所定義的要求，且佐證主要網路視角的遠端網路視角分別位於至少 2 個不同的區域網際網路註冊管理機構（Regional Internet Registries）服務區域內。若未符合該等要求，則 CA **不得（MUST NOT）**繼續簽發憑證。
- 自 2026-12-15 起：CA **應（MUST）**使用至少 5 個遠端網路視角進行多視角簽發佐證。CA **應（MUST）**確保符合《法定數量要求表》所定義的要求，且佐證主要網路視角的遠端網路視角分別位於至少 2 個不同的區域網際網路註冊管理機構（Regional Internet Registries）服務區域內。若未符合該等要求，則 CA **不得（MUST NOT）**繼續簽發憑證。

### 3.2.3 個人身分之鑑別

若適用本文件第 3.2.3 節規定之申請者（Applicant）為自然人，憑證機構（Certification Authority，CA）**應（SHALL）**驗證該申請者的姓名、地址，以及憑證申請的真實性。

CA **應（SHALL）**使用至少一份目前有效且由政府核發之附照片身分證明文件（護照、駕照、軍人身分證、國民身分證或同等類型文件）的清晰副本，且該副本必須能清楚辨識申請者的面貌，以驗證申請者的姓名。CA **應（SHALL）**檢查該副本是否有任何遭竄改或偽造的跡象。

CA **應（SHALL）**使用其認定為可靠的身分證明文件，例如政府核發之身分證明文件、公用事業費用帳單，銀行對帳單或信用卡帳單，以驗證申請者的地址。CA **得（MAY）**使用與驗證申請者姓名相同的政府核發之身分證明文件驗證申請者地址。

CA **應（SHALL）**使用可靠通訊方式（Reliable Method of Communication）與申請者確認該憑證申請。

### 3.2.4 未經驗證的用戶資訊

### 3.2.5 組織授權之驗證

若申請者（Applicant）申請之憑證包含主體識別資訊（Subject Identity Information），且申請者為組織，則憑證機構（Certification Authority，CA）**應（SHALL）**使用可靠通訊方式（Reliable Method of Communication）驗證申請者代表（Applicant Representative）所提出之憑證申請的真實性。

CA **得（MAY）**使用第 3.2.2.1 節所列之來源，確認申請者的可靠通訊方式。在使用可靠通訊方式的前提下，CA **得（MAY）**直接向申請者代表或申請者組織內的權威來源（authoritative source；例如申請者的主要營業處所、公司辦事處、人力資源部門、資訊科技部門，或 CA 認為適當的其他單位）確認憑證申請的真實性。

此外，CA **應（SHALL）**建立一個流程，允許申請者指定有權提出憑證申請之人員。若申請者以書面方式指定可提出憑證申請之人員，則 CA **不得（SHALL NOT）**接受任何超出該指定範圍之憑證申請。CA **應（SHALL）**於收到已確認其真實性之申請者書面請求時，向申請者提供其所授權之憑證申請人員清單。

### 3.2.6 交互運作或交互認證之準則
憑證機構（Certification Authority，CA）**應（SHALL）**公開揭露所有以憑證機構自身為主體（Subject）的交互認證之下屬憑證機構憑證（Cross-Certified Subordinate CA Certificate），前提是憑證機構自身安排或接受建立該憑證信賴關係（即本節所述的交互認證之下屬憑證機構憑證）。

## 3.3 金鑰更換請求之識別與鑑別

### 3.3.1 例行性金鑰更換之識別與鑑別

### 3.3.2 憑證廢止後金鑰更換之識別與鑑別

## 3.4 憑證廢止請求之識別與鑑別

---

# 4 憑證生命週期作業要求

## 4.1 憑證申請

### 4.1.1 可提出憑證申請之人
不作規定。

### 4.1.2 申辦流程與責任
在簽發憑證前，憑證機構（Certification Authority，CA）**應（SHALL）**向申請者（Applicant）取得以下文件：

1. 憑證申請書，可以是電子形式；以及

2. 已簽署之用戶協議（Subscriber Agreement）或使用條款（Terms of Use），可以是電子形式。

CA **宜（SHOULD）**取得其認定為符合本文件要求規定所需之任何其他文件。

在簽發憑證前，CA **應（SHALL）**向申請者取得依 CA 規定格式提出，且遵循本文件要求規定之憑證申請。同一份憑證申請**得（MAY）**作為簽發多張憑證給同一申請者之依據，但應符合第 4.2.1 節規定之時效與更新要求，且每張憑證應由適當之申請者代表（Applicant Representative）代表申請者簽署一份現行有效的憑證申請書作為依據。憑證申請書**得（MAY）**以電子形式製作、提出及／或簽署。

憑證申請**應（MUST）**包含由申請者或其代表提出之憑證簽發請求，以及由申請者或其代表對所載之所有資訊均屬正確之聲明。

## 4.2 憑證申請之處理

### 4.2.1 執行識別與鑑別作業

憑證申請**得（MAY）**包含擬記載於憑證中之所有與申請者（Applicant）相關的事實資料，以及憑證機構（Certification Authority，CA）為了遵循本文件要求規定及其憑證政策（Certificate Policy，CP）及／或憑證實務作業基準（Certification Practice Statement，CPS）而有必要向申請者取得之其他資訊。若憑證申請未包含全部所需的申請者資訊，CA **應（SHALL）**向申請者取得其餘所需資訊，或先從可靠且獨立的第三方資料來源取得該資訊，再向申請者確認其內容。CA **應（SHALL）**建立並遵從書面程序，以驗證申請者要求記載於憑證中的所有資料。

申請者資訊**應（MUST）**包括（但不限於）至少一個將記載於憑證 `subjectAltName` 擴充欄位中的完全吻合網域名稱（Fully-Qualified Domain Name，FQDN）或 IP 位址（IP Address）。

第 6.3.2 節限制用戶憑證（Subscriber Certificates）的有效期。

CA **得（MAY）**使用第 3.2 節規定的文件與資料驗證憑證資訊，或重複使用先前已完成的驗證成果（包括組織授權之驗證），前提是 CA 簽發憑證前，應於下表所定之最大天數內，自第 3.2 節規定之來源取得資料或文件，或 CA 已完成的驗證成果：

| 憑證於此日或之後簽發 | 憑證於此日前簽發 | 可重複使用已驗證資料之最長期限 |
|---|---|---|
| | 2026-03-15 | 825 日 |
| 2026-03-15 | | 398 日 |

可重複使用主體識別資訊已驗證資料之最長期限

依第 3.2.2.4 節與第 3.2.2.5 節進行的網域名稱（Domain Name）及 IP 位址驗證，其所使用之任何資料、文件或完成的驗證成果，**應（MUST）**於簽發憑證前，於下表所定之最大天數內取得：

| 憑證於此日或之後簽發 | 憑證於此日前簽發 | 可重複使用已驗證資料之最大期限 |
|---|---|---|
| | 2026-03-15 | 398 日 |
| 2026-03-15 | 2027-03-15 | 200 日 |
| 2027-03-15 | 2029-03-15 | 100 日 |
| 2029-03-15 | | 10 日 |

可重複使用網域名稱及 IP 位址已驗證資料之最長期限

若先前驗證所使用之任何資料或文件，其取得日期於簽發憑證前已超過可重複使用已驗證資料之最長期限，則不得於任何情況下重複使用先前的已驗證成果。

於《基本要求》或《EV 指引》所規定之任何驗證方法發生變更後，CA 可繼續重複使用變更前所蒐集的驗證資料或文件，或先前完成的已驗證成果，其可重複使用期限依第 4.2.1 節規定辦理；除非投票案（Ballot）另有明文規定。

CA **應（SHALL）**建立、維護並實施書面程序，以識別高風險憑證申請（High Risk Certificate Request），並於核准憑證前要求執行額外的驗證作業；該等程序應於合理且必要之範圍內，確保此類申請均依本文件要求規定完成妥善驗證。

若受委任第三方（Delegated Third Party）履行 CA 於本節所規定之任何義務，CA **應（SHALL）**確認受委任第三方用以識別及進一步驗證的高風險憑證申請之流程，其所提供的保證等級至少與 CA 自身流程相同。

### 4.2.2 憑證申請之核准或拒絕

憑證機構（Certification Authority，CA）**不得（SHALL NOT）**簽發含有內部名稱（Internal Name）或保留 IP 位址（Reserved IP Address）之憑證，因其無法依第 3.2.2.4 節或第 3.2.2.5 節之規定完成驗證。

自 2026-03-15 起，CA **不得（SHALL NOT）**簽發其所含網域名稱係以 IP 反向區域後綴（IP Reverse Zone Suffix）結尾之憑證。

#### 4.2.2.1 授權憑證機構簽發憑證（CAA）紀錄之處理

作為憑證簽發流程的一部分，憑證機構（Certification Authority，CA）**應（MUST）**針對 `subjectAltName` 擴充欄位中不包含 Onion 網域名稱（Onion Domain Name）之每個 `dNSName`，依據 RFC 8659 取得並處理 CAA 紀錄。這些實務作業**應（MUST）**於 CA 的憑證政策（Certificate Policy，CP）及／或憑證實務作業基準（Certification Practice Statement，CPS）第 4.2 節中說明，其中應具體包含該 CA 於 CAA 「issue」或「issuewild」紀錄中所認可、並允許其簽發憑證之簽發者網域名稱（Issuer Domain Names）集合。

CA **得（MAY）**在任何其他時間檢查 CAA 紀錄。

當處理 CAA 紀錄時，CA **應（MUST）**依據 RFC 8659 之規定解析並處理 issue、issuewild 與 iodef 屬性標籤，但不要求對 iodef 屬性標籤的內容採取任何動作。CA **得（MAY）**支援額外的屬性標籤，但**不得（MUST NOT）**與本文件所規定的強制性屬性標籤發生衝突，或凌駕於其上。CA **應（MUST）**遵守關鍵性

旗標（critical flag）之要求，若遇到設有該旗標之無法識別的屬性標籤，不得簽發憑證。

若 CA 處理 CAA 紀錄完成後要簽發憑證，**應（MUST）**在 CAA 紀錄的 TTL（Time to Live）設定值或 8 小時內（以時間較長者為準）簽發憑證。

RFC 8659 要求 CA「除非 CA 判定下列任一情況成立，否則**不得（MUST NOT）**簽發憑證（1）憑證申請符合適用的 CAA 資源記錄集（CAA Resource Record Set，CAA RRset）；或（2）適用相關憑證政策（CP）或憑證實務作業基準（CPS）所規定之例外情況。」。對於依據本《基本要求》規定所簽發之憑證，CA **不得（MUST NOT）**援用其 CP 或 CPS 所規定之任何例外情況，除非該例外情況為以下情形之一：

- 已產生憑證透明度預簽憑證（Certificate Transparency Precertificate，參見第 7.1.2.9 節）、且該預簽憑證登錄於至少兩個公開記錄系統，以及在簽發預簽憑證時已完成 CAA 檢查之憑證，無須再次執行 CAA 檢查。
- 依第 7.1.2.3 節或第 7.1.2.5 節規定的受技術約束之下屬憑證機構憑證（Technically Constrained Subordinate CA Certificate）所簽發之憑證，若與申請者的契約中已明文約定不執行 CAA 檢查，則無須再次執行 CAA 檢查。

於下列情況，允許 CA 將 CAA 檢查失敗視為許可簽發：

- 查詢失敗發生於 CA 的基礎設施之外；且
- 查詢已重試至少 1 次；且
- CA 已確認該網域符合 RFC 4035 第 4.3 節 定義的「Insecure」（未受 DNSSEC 保護）。

CA **應（MUST）**以書面文件記錄因 CAA 紀錄而中止的憑證簽發，以便向 CA/Browser Forum 提供相關情況的回饋，若 CAA iodef 紀錄存在，**宜（SHOULD）**將此類簽發申請的相關報告傳送至該紀錄中所指定之聯絡人。CA 無須支援 iodef 紀錄中 mailto: 或 https: 以外的 URL 協定。

由主要網路視角（Primary Network Perspective）執行之 CAA 紀錄檢查相關的所有 DNS 查詢，**應（MUST）**依據第 4.2.2.2 節執行 DNSSEC 驗證。

#### 4.2.2.1.1 授權憑證機構簽發憑證（CAA）之多視角簽發佐證

某些用於驗證申請者（Applicant）對憑證中所列主體網域名稱（subject domain(s)）（參見第 3.2.2.4 節）或 IP 位址（IP Address）（參見第 3.2.2.5 節）之所有權或控管權的方法，要求在憑證簽發前，從其他的遠端網路視角（remote Network Perspective）取得並處理 CAA 紀錄（參見第 3.2.2.9 節）。為了佐證主要網路視角（Primary Network Perspective），遠端網路視角的 CAA 檢查結果**應（MUST）**被解釋為許可才能簽發，無論來自這兩個視角的回應結果是否每個位元組都相同。此外，若其中一個或兩個視角遇到第 4.2.2.1 節所定義的可接受 CAA 紀錄檢查失敗，CA **得（MAY）**將來自遠端網路視角的回應視為有效佐證。

#### 4.2.2.1.2 授權憑證機構簽發憑證（CAA）之參數

處理 CAA 紀錄時，憑證機構（Certification Authority，CA）**宜（SHOULD）**依 RFC 8657 之規定處理 `accounturi` 與 `validationmethods` 參數。

*自 2027-03-15 起*，處理 CAA 紀錄時，CA **應（MUST）**依 RFC 8657 之規定處理 `accounturi` 與 `validationmethods` 參數。

此外，*自 2027-03-15 起*：

- 若 CA 未依 RFC 8555 所述，以 ACME Account URL 識別憑證用戶的帳號，CA **應（MUST）**於其憑證政策（CP）及／或憑證實務作業基準（CPS）第 4.2 節中定義其所支援的 `accounturi` 格式，並**宜（SHOULD）**遵循 RFC 7565 所定義的「acct」URI scheme。
- 對於使用 ACME 協定提出的憑證申請，CA **得（MAY）**允許 `accounturi` 參數指定主要組織帳號（「父帳號」（Parent Account））。作為 RFC 8657 第 3 節之明確例外，若且唯若（if and only if）CA 確保下列各項均成立，CA **得（MAY）**簽發由另一帳號（「下屬 ACME 帳號」（Subordinate ACME Account））所申請之憑證：
  1. CA 維護一份內部且可供稽核之對應關係，將下屬 ACME 帳號繫結至 `accounturi` 所指定的父帳號。
  2. CA 已透過密碼學方式或管理程序驗證，父帳號已明確授權下屬 ACME 帳號依此對應關係取得憑證。
  3. CA 於本文件所規定之標準資料保存期限內，保存足以證明此項授權及對應關係的稽核紀錄。
- 若 CA 支援未登記於 IANA ACME Validation Methods registry 的網域驗證方法，CA **應（MUST）**解析並處理由字串「ca-tbr-」與《基本要求》第 3.2.2.4 節之小節編號所串接而成的 `validationmethods` 標籤，例如「ca-tbr-7」代表《基本要求》第 3.2.2.4.7 節所述之 DNS 方法。若 CA 使用可由不同標籤表示的機制執行網域驗證（例如「http-01」與「ca-tbr-19」），CA **宜（SHOULD）**將其中任一標籤視為授權簽發憑證的驗證方法。
- `validationmethods` 標籤的規範表示形式為小寫字母。但 CA **得（MAY）**以不區分大小寫（case insensitive）之方式比對標籤。若 CA 確實採用不區分大小寫的標籤比對方式，此項實務作業**應（MUST）**記載於其憑證政策（CP）及／或憑證實務作業基準（CPS）中。

#### 4.2.2.2 DNSSEC 驗證之要求

本節整合所有適用於網域驗證（第 3.2.2.4 節）及 CAA 紀錄之處理（第 4.2.2.1 節）過程中所執行之 DNS 查詢的 DNSSEC 驗證要求。

##### 4.2.2.2.1 DNS 解析器之要求

主要網路視角（Primary Network Perspective）用於網域授權或控管權驗證相關的所有 DNS 查詢及 CAA 紀錄檢查之 DNS 解析器（DNS resolver），**應（MUST）**：

- 使用 RFC 4035 第 5 節 定義的演算法執行 DNSSEC 驗證；且
- 支援 RFC 5155 定義的 NSEC3；且
- 支援 RFC 4509 與 RFC 5702 定義的 SHA-2；且
- 妥善處理 RFC 6840 第 4 節 所列舉的安全疑慮。

#### 4.2.2.2.2 適用性與範圍

主要網路視角（Primary Network Perspective）**應（MUST）**對與下列事項相關的所有 DNS 查詢執行 DNSSEC 驗證：

1. 第 3.2.2.4 節所述之網域授權或控管權驗證；且
2. 第 4.2.2.1 節所述之 CAA 紀錄檢查。

#### 4.2.2.2.3 電子郵件之網域驗證方法 - 部分例外

對於第 3.2.2.4.4 節、第 3.2.2.4.13 節與第 3.2.2.4.14 節內容所述之使用電子郵件（e-mail）為基礎的網域驗證方法：

- 主要網路視角（Primary Network Perspective）為了取得經授權網域名稱（Authorization Domain Name，ADN）所執行的所有 DNS CNAME、CAA 與 TXT 查詢，**應（MUST）**執行 DNSSEC 驗證，且 CA **不得（MUST NOT）**利用內部政策對該等查詢停用 DNSSEC 驗證。
- 對於主要網路視角執行之與該等方法相關的所有其他 DNS 查詢，**宜（SHOULD）**執行 DNSSEC 驗證，且 CA **不宜（SHOULD NOT）**利用內部政策停用 DNSSEC 驗證。

#### 4.2.2.2.4 禁止停用 DNSSEC 驗證

對於第 4.2.2.2.3 節所列之範圍外的所有網域驗證方法，以及所有 CAA 紀錄檢查，CA **不得（MUST NOT）**針對主要網路視角（Primary Network Perspective）執行之任何與網域授權或控管權驗證相關、或與 CAA 紀錄檢查相關的 DNS 查詢，利用內部政策停用 DNSSEC 驗證。

#### 4.2.2.2.5 DNSSEC 驗證錯誤

除第 4.2.2.2.3 節可能允許之情形外，由主要網路視角（Primary Network Perspective）觀察到的 DNSSEC 驗證錯誤（例如：SERVFAIL）**不得（MUST NOT）**被視為許可簽發之依據。

#### 4.2.2.2.6 遠端網路視角

作為多視角簽發佐證（Multi-Perspective Issuance Corroboration）的一部分，**得（MAY）**針對由遠端網路視角（Remote Network Perspectives）執行之與網域授權或控管權驗證相關、以及與 CAA 紀錄檢查相關的所有 DNS 查詢，執行信賴鏈串鏈至 IANA DNSSEC 信賴根源（IANA DNSSEC root trust anchor）的 DNSSEC 驗證。

#### 4.2.2.2.7 排除事項

與 DNSSEC 驗證相關之完整 DNS 查詢資訊，不屬於下列要求的適用範圍：

1. 為符合第 8.7 節要求而執行的內部稽核（self-audits）；且
2. 第 5.4.1 節的紀錄要求（logging requirements）規定。

儘管有上述排除事項，CA 仍**應（MUST）**保存充足資訊，以驗證 DNSSEC 驗證是依第 4.2.2.2 節其餘要求所執行。

### 4.2.3 憑證申請之處理時間
不作規定。

## 4.3 憑證簽發

### 4.3.1 憑證簽發期間憑證機構之作業

#### 4.3.1.1 根憑證機構憑證簽發之人工授權
根憑證機構（Root CA）簽發憑證時，**應（SHALL）**要求經憑證機構（Certification Authority，CA）授權之人員（即 CA 系統操作員、系統管理員或 PKI 管理員）明確地下達直接指令，Root CA 始得執行憑證簽章作業。

#### 4.3.1.2 待簽章憑證內容之 Linting（語法檢查）
由於實作符合本文件要求規定的憑證剖繪（Certificate Profiles）具有相當複雜性，憑證機構（Certification Authority，CA）於簽章每個待簽章物件前，實作 Linting 流程以檢查其技術符合性，被視為最佳實務。當預簽憑證（Precertificate）已完成 Linting 時，若 CA 具備技術控管措施，可依據 RFC 6962 第 3.2 節 所述方式驗證待簽章憑證與待簽章預簽憑證之間的對應關係，則相對應待簽章憑證無須進行 Linting。

自 2025-03-15 起，CA **應（SHALL）**實作此類 Linting 流程。

用於產生包含待簽章憑證內容之憑證的方法包括但不限於：

1. 使用「虛設（Dummy）」私密金鑰（Private Key）對 `tbsCertificate` 進行簽章，而該私密金鑰的公開金鑰（Public Key）元件未經憑證鏈串鏈至公開信賴 CA 憑證之憑證所認證；或
2. 於憑證 ASN.1 SEQUENCE 的 `signature` 欄位指定固定值。

CA **得（MAY）**實作自有的憑證 Linting 工具，但 CA **宜（SHOULD）**使用業界廣泛採用的 Linting 工具（參見 https://cabforum.org/resources/tools/）。

鼓勵 CA 對開源 Linting 專案做出貢獻，例如：

- 新增 lint 或改善既有的 lint，
- 將可能不正確的 linting 結果作為缺陷（bug）回報，
- 通知 Linting 軟體維護者現有 lint 尚未涵蓋的檢查項目，
- 更新既有 lint 的說明文件，以及
- 產製供特定 lint 進行正向／負向測試（positive/negative tests）的測試憑證。

#### 4.3.1.3 已簽發憑證之 Linting（語法檢查）
憑證機構（Certification Authority，CA）**得（MAY）**使用 Linting 流程檢查每張已簽發的憑證。

### 4.3.2 憑證機構通知用戶憑證已簽發
不作規定。

## 4.4 憑證接受

### 4.4.1 構成接受憑證之行為
不作規定。

### 4.4.2 憑證機構對簽發憑證之發布
不作規定。

### 4.4.3 憑證機構通知其他實體憑證已簽發
不作規定。

## 4.5 金鑰對與憑證之使用

### 4.5.1 用戶私密金鑰與憑證之使用
參見第 9.6.3 節第 2 項及第 4 項規定。

### 4.5.2 信賴憑證者公開金鑰與憑證之使用
不作規定。

## 4.6 憑證展期

### 4.6.1 憑證展期之情況
不作規定。

### 4.6.2 可申請憑證展期之人
不作規定。

### 4.6.3 憑證展期申請之處理
不作規定。

### 4.6.4 通知用戶展期後的新憑證已簽發
不作規定。

### 4.6.5 構成接受展期後的憑證之行為
不作規定。

### 4.6.6 憑證機構對展期後的憑證之發布
不作規定。

### 4.6.7 憑證機構通知其他實體展期後的憑證已簽發
不作規定。

## 4.7 憑證金鑰更換

### 4.7.1 憑證金鑰更換之情況
不作規定。

### 4.7.2 可請求憑證更換公開金鑰之人
不作規定。

### 4.7.3 憑證金鑰更換請求之處理
不作規定。

### 4.7.4 通知用戶更換金鑰的新憑證已簽發
不作規定。

### 4.7.5 構成接受更換金鑰的憑證之行為
不作規定。

### 4.7.6 憑證機構對更換金鑰的憑證之發布
不作規定。

### 4.7.7 憑證機構通知其他實體更換金鑰的憑證已簽發
不作規定。

## 4.8 憑證變更

### 4.8.1 憑證變更之狀況
不作規定。

### 4.8.2 可請求憑證變更之人
不作規定。

### 4.8.3 憑證變更請求之處理
不作規定。

### 4.8.4 通知用戶變更後的新憑證已簽發
不作規定。

### 4.8.5 構成接受變更後的憑證之行為
不作規定。

### 4.8.6 憑證機構對變更後的憑證之發布
不作規定。

### 4.8.7 憑證機構通知其他實體變更後的憑證已簽發
不作規定。

## 4.9 憑證廢止與暫時停用

### 4.9.1 憑證廢止之情況

#### 4.9.1.1 廢止用戶憑證之事由
憑證機構（Certification Authority，CA）**得（MAY）**支援廢止短效期用戶憑證（Short-lived Subscriber Certificate）。

除短效期用戶憑證外，若發生下列一項或多項情形時，CA **應（SHALL）**於 24 小時內廢止憑證，並使用對應之 CRLReason（參見第 7.2.2 節）：

1. 用戶以書面方式請求 CA 廢止憑證，且未指定 CRLReason（CRLReason 為「unspecified (0)」，因此憑證廢止清冊（Certificate Revocation List，CRL）中不會包含 reasonCode 擴充欄位）；
2. 用戶通知 CA，其原始憑證申請未經授權，且不溯及既往補予授權（CRLReason #9，privilegeWithdrawn）；
3. CA 取得證據，顯示用戶憑證中的公開金鑰（Public Key），其所對應之私密金鑰（Private Key）遭破解（Key Compromise）（CRLReason #1，keyCompromise）；
4. CA 獲悉已有經展示或證實之方法，可依據憑證中的公開金鑰輕易計算出與其對應之用戶私密金鑰，包括但不限於第 6.1.1.3(5) 節中所列之方法（CRLReason #1，keyCompromise）；
5. CA 取得證據，顯示憑證中任何完全吻合網域名稱（Fully-Qualified Domain Name，FQDN）或 IP 位址（IP Address）之網域授權或控管權驗證結果不可被信賴，包括 CA 未正確執行 CAA 檢查，或依第 3.2.2.8 節（CAA Records）之規定不被許可簽發該憑證之情況（CRLReason #4，superseded）。

除短效期用戶憑證外，若發生下列一項或多項情形時，CA **宜（SHOULD）**於 24 小時內廢止憑證，且最遲**應（MUST）**於 5 日內完成廢止，並使用對應之 CRLReason（參見第 7.2.2 節）：

6. 該憑證已不再遵循第 6.1.5 節與第 6.1.6 節之規定（CRLReason #4，superseded）；
7. CA 取得證據，顯示憑證遭誤用（CRLReason #9，privilegeWithdrawn）；
8. CA 獲悉用戶違反其依用戶協議（Subscriber Agreement）或使用條款（Terms of Use）所負之一項或多項重大義務（CRLReason #9，privilegeWithdrawn）；
9. CA 獲悉任何足以顯示憑證中所載之完全吻合網域名稱（FQDN）或 IP 位址已不再依法得以使用之情況（例如：法院或仲裁人已撤銷網域名稱註冊人使用該網域名稱之權利）（CRLReason #5，cessationOfOperation）；
10. CA 獲悉某張萬用網域憑證（Wildcard Certificate）已被用於驗證具有詐欺性誤導之該萬用網域 FQDN 的子網域（Subordinate FQDN）網站（CRLReason #9，privilegeWithdrawn）；
11. CA 獲悉憑證所載之資訊發生重大變更（CRLReason #9，privilegeWithdrawn）；
12. CA 獲悉該憑證未依據本文件要求規定、CA 的憑證政策（Certificate Policy，CP）或憑證實務作業基準（Certification Practice Statement，CPS）（CRLReason #4，superseded）簽發；
13. CA 判定或獲悉憑證所載之任何資訊有誤（CRLReason #9，privilegeWithdrawn）；
14. CA 依《基本要求》簽發憑證之權利到期、遭撤銷或終止，除非 CA 已作好安排以持續維護 CRL/OCSP 儲存庫（CRLReason 為「unspecified (0)」，因此 CRL 中不會包含 reasonCode 擴充欄位）；

15. 依 CA 的憑證政策（CP）及／或憑證實務作業基準（CPS），因本文件第 4.9.1.1 節未另行規定之原因而必須廢止憑證（CRLReason 為「unspecified (0)」，因此 CRL 中不會包含 reasonCode 擴充欄位）；或

16. CA 獲悉已有經展示或證實之方法，足以導致用戶的私密金鑰遭破解，或有明確證據顯示用於產製該私密金鑰之特定方法存在缺陷（CRLReason #1，keyCompromise）。

#### 4.9.1.2 廢止下屬憑證機構憑證之事由

若發生下列一項或多項情形時，簽發憑證機構（Issuing CA）**應（SHALL）**於 7 日內廢止下屬憑證機構（Subordinate CA）憑證：

1. 下屬憑證機構以書面方式請求廢止；

2. 下屬憑證機構通知簽發憑證機構，其原始憑證申請未經授權，且不溯及既往補予授權；

3. 簽發憑證機構取得證據，顯示下屬憑證機構憑證中的公開金鑰（Public Key），其所對應之私密金鑰（Private Key）遭破解（Key Compromise），或已不再遵循第 6.1.5 節與第 6.1.6 節之規定；

4. 簽發憑證機構取得證據，顯示憑證遭誤用；

5. 簽發憑證機構獲悉該憑證未依據本文件規定簽發；或下屬憑證機構未遵循本文件規定、或者未遵循適用之憑證政策（Certificate Policy，CP）或憑證實務作業基準（Certification Practice Statement，CPS）；

6. 簽發憑證機構判定憑證所載之任何資訊有誤或具誤導性；

7. 簽發憑證機構或下屬憑證機構因任何原因停止營運，且未安排其他 CA 為憑證提供廢止狀態服務；

8. 簽發憑證機構或下屬憑證機構依《基本要求》簽發憑證之權利到期、遭撤銷或終止，除非簽發憑證機構已作好安排以持續維護 CRL/OCSP 儲存庫；或

9. 依簽發憑證機構的憑證政策（CP）及／或憑證實務作業基準（CPS），必須廢止該憑證。

### 4.9.2 可請求憑證廢止之人

用戶（Subscriber）、註冊機構（Registration Authority，RA）或簽發憑證機構（Issuing CA）可發起憑證廢止。此外，用戶、信賴憑證者（Relying Party）、應用軟體供應商（Application Software Supplier）及其他第三方可提出憑證問題報告（Certificate Problem Report），通知簽發憑證機構該憑證具有合理廢止的事由。

### 4.9.3 憑證廢止請求之程序

憑證機構（Certification Authority，CA）**應（SHALL）**提供用戶（Subscriber）請求廢止其自身憑證（Certificate）之流程。該流程**應（MUST）**於 CA 的憑證政策（Certificate Policy，CP）或憑證實務作業基準（Certification Practice Statement，CPS）中說明。CA **應（SHALL）**持續維持每週 7 天、每天 24 小時（24x7）接受並處理廢止請求與憑證問題報告（Certificate Problem Report）之能力。

CA **應（SHALL）**向用戶、信賴憑證者（Relying Party）、應用軟體供應商（Application Software Supplier）及其他第三方提供明確的指示，以供回報疑似私密金鑰遭破解（Private Key Compromise）、憑證誤用（Certificate misuse），或其他類型之詐欺、遭破解、誤用、不當行為，或任何其他與憑證相關之事項。CA **應（SHALL）**透過易於取得之線上方式及其憑證實務作業基準（CPS）第 1.5.2 節中公開揭露該等指示。

### 4.9.4 憑證廢止請求之寬限期

不作規定。

### 4.9.5 憑證機構處理憑證廢止請求之期限

憑證機構（Certification Authority，CA）**應（SHALL）**於收到憑證問題報告（Certificate Problem Report）後 24 小時內，調查與憑證問題報告相關的事實與情況，並向用戶（Subscriber）及提出該憑證問題報告之實體提供其調查結果之初步報告。

在審查相關事實與情況後，CA **應（SHALL）**與用戶及提出憑證問題報告或其他提出憑證廢止相關通知之任何實體合作，以確認是否廢止憑證；如應予廢止，應同步確定 CA 廢止該憑證之日期。自收到憑證問題報告或憑證廢止相關通知起，至公布憑證廢止之期間，**不得（MUST NOT）**超過第 4.9.1.1 節所規定之時限。CA 於決定廢止日期時，**宜（SHOULD）**考慮以下因素：

1. 所指稱問題之性質（包括其範圍、背景、嚴重程度、影響規模及造成危害之風險）；
2. 憑證廢止之後果（對用戶及信賴憑證者（Relying Party）的直接及附加影響）；
3. 收到針對特定憑證或用戶之憑證問題報告數量；
4. 提出投訴之實體（例如，執法人員提出某網站從事非法活動之投訴，相較於消費者主張未收到其所訂購商品之投訴，應給予較高之權重）；以及
5. 相關法令。

### 4.9.6 信賴憑證者之憑證廢止狀態檢查規定

不作規定。

**注意**：憑證於簽發後，憑證可能因第 4.9 節所列之原因而遭廢止。因此，信賴憑證者宜檢查所有包含 CDP 或 OCSP 指示資訊之憑證的廢止狀態。

### 4.9.7 憑證廢止清冊之簽發頻率

憑證廢止清冊（Certificate Revocation List，CRL）**應（MUST）**可透過能公開存取之 HTTP URL 取得（即視為「已發布（published）」）。

憑證機構（Certification Authority，CA）**應（MUST）**於簽發其第一張憑證後 24 小時內，產生並發布下列任一項：

- 完整 CRL（full and complete CRL）；或
- 分割式（即「分片（sharded）」）CRL，其全部分片彙整後應相當於一份完整 CRL。

簽發用戶憑證（Subscriber Certificates）之憑證機構：

1. **應（MUST）**至少每隔下列期間更新並發布新的憑證廢止清冊（CRL）：
   - 若所有憑證均包含其 accessMethod 為 `id-ad-ocsp` 之憑證機構資訊存取（Authority Information Access，AIA）擴充欄位（「AIA OCSP 指示資訊」），則為 7 日；或
   - 其他所有情況下為 4 日；
2. **應（MUST）**於憑證記為已廢止後 24 小時內更新並發布新的 CRL。

簽發 CA 憑證之憑證機構：

1. **應（MUST）**至少每 12 個月更新並發布新的 CRL；
2. **應（MUST）**於憑證記為已廢止後 24 小時內更新並發布新的 CRL。

憑證機構**應（MUST）**持續發布 CRL，直到下列任一情況成立：

- 所有包含相同主體公開金鑰（Subject Public Key）之下屬憑證機構（Subordinate CA）憑證均已到期或遭廢止；或
- 對應之下屬憑證機構私密金鑰已銷毀。

### 4.9.8 憑證廢止清冊發布之最大延遲時間（如適用）

不作規定。

### 4.9.9 線上憑證廢止與狀態檢查之可用性

線上憑證狀態協定（Online Certificate Status Protocol，OCSP）回應之效期區間為 `thisUpdate` 與 `nextUpdate` 欄位間之時間差（包含 `thisUpdate` 與 `nextUpdate`）。計算時間差的時候，3,600 秒應視為 1 小時，86,400 秒應視為 1 日，不考慮閏秒。

憑證序號符合下列情形之一者，視為「已分配（assigned）」：

- 具有該序號之憑證或預簽憑證（Precertificate）已由簽發憑證機構（Issuing CA）簽發；或
- 具有該序號之預簽憑證已由簽發憑證機構（Issuing CA）關聯之預簽憑證簽章憑證（Precertificate Signing Certificate，如第 7.1.2.4 節所定義）簽發。

憑證序號若非屬「已分配」，則視為「未分配（unassigned）」。

對於包含 accessMethod 為 `id-ad-ocsp` 之憑證機構資訊存取（Authority Information Access, AIA）擴充欄位的憑證及預簽憑證（Precertificate），其狀態資訊之提供**應（SHALL）**符合以下規定。

由 CA 營運之 OCSP 回應伺服器（OCSP Responder）**應（SHALL）**支援 HTTP GET 方法，如 RFC 6960 及／或 RFC 5019 所述。CA **得（MAY）**依 RFC 8954 處理 Nonce 擴充欄位（1.3.6.1.5.5.7.48.1.2）。

關於用戶憑證或其對應預簽憑證之狀態：

- 自 2025-01-15 起，權威性 OCSP 回應**應（MUST）**自憑證或預簽憑證首次發布或以其他方式提供後，不超過 15 分鐘即可取得（即回應伺服器**不得（MUST NOT）**回覆「unknown」狀態）。
- 對於效期區間不足 16 小時之 OCSP 回應，CA **應（SHALL）**於距離 `nextUpdate` 尚有半個效期區間的時間前，提供已更新之 OCSP 回應。
- 對於效期區間不低於 16 小時之 OCSP 回應，CA **應（SHALL）**至少於 `nextUpdate` 前 8 小時提供已更新之 OCSP 回應，且不得晚於 `thisUpdate` 後 4 日。

關於下屬憑證機構憑證（Subordinate CA Certificate）之狀態，CA **應（SHALL）**至少每 12 個月提供一次已更新之 OCSP 回應，並應於廢止該憑證後 24 小時內提供已更新之 OCSP 回應。

對於 OCSP 回應伺服器願意或必須回覆之**所有**憑證，其狀態資訊之提供**應（SHALL）**符合下列規定。

OCSP 回應**應（MUST）**符合 RFC 6960 及／或 RFC 5019。OCSP 回應**應（MUST）**符合下列任一情況：

1. 由簽發其廢止狀態接受查詢之憑證的 CA 簽章 OCSP 回應；或
2. 由遵循第 7.1.2.8 節 OCSP 回應伺服器憑證剖繪之 OCSP 回應伺服器簽章 OCSP 回應。

用戶憑證之 OCSP 回應，其效期區間**應（MUST）**不低於 8 小時且不超過 10 日。

若 OCSP 回應伺服器收到的查詢屬於「未分配」憑證序號狀態的請求，則回應伺服器**不宜（SHOULD NOT）**以「good」狀態回覆。若該 OCSP 回應伺服器所屬之 CA 並未依第 7.1.2.3 節或第 7.1.2.5 節受技術約束（Technically Constrained），則回應伺服器對此類請求**不得（MUST NOT）**以「good」狀態回覆。

### 4.9.10 線上憑證廢止狀態檢查之要求

不作規定。

### 4.9.11 其他可用之憑證廢止資訊發布方式

不作規定。

### 4.9.12 金鑰遭破解時之特別要求

參見第 4.9.1 節。

### 4.9.13 憑證暫時停用之情況
儲存庫（Repository）**不得（MUST NOT）**包含任何顯示憑證處於暫時停用（Suspend）狀態的項目。

### 4.9.14 可請求憑證暫時停用之人
不適用。

### 4.9.15 憑證暫時停用請求之程序
不適用。

### 4.9.16 憑證暫時停用期間之限制
不適用。

## 4.10 憑證狀態服務

### 4.10.1 服務特性
於已廢止憑證之到期日前，**不得（MUST NOT）**移除憑證廢止清冊（CRL）或線上憑證狀態協定（OCSP）回應中之該憑證廢止資訊。

### 4.10.2 服務可用性
憑證機構（Certification Authority，CA）**應（SHALL）**以充足之資源營運及維護其憑證廢止清冊（CRL）及其選擇提供之線上憑證狀態協定（OCSP）功能，以確保在正常營運狀況下，其回應時間為 10 秒或更短。

CA **應（SHALL）**維護每週 7 天、每天 24 小時（24x7）均可存取之線上儲存庫（Repository），供應用軟體使用，以自動檢查該 CA 所簽發之所有未到期憑證的目前狀態。

CA **應（SHALL）**持續維持每週 7 天、每天 24 小時（24x7）之回應機制，以處理高優先權之憑證問題報告（Certificate Problem Report），並於適當時機將此類投訴轉交執法機關，及／或廢止該投訴所涉及之憑證。

### 4.10.3 選用性功能
不作規定。

## 4.11 服務關係終止
不作規定。

## 4.12 金鑰代管與復原

### 4.12.1 金鑰代管與復原之政策與實務
不作規定。

### 4.12.2 Session key（對話鍵）封裝與復原之政策及實務
不適用。

---

# 5 管理、作業及實體控管
CA/Browser Forum《網路與憑證系統安全要求》（Network and Certificate System Security Requirements）以引用方式納入本文件，其內容視同已全文載明於本文件。

憑證機構（Certification Authority，CA）**應（SHALL）**建立、實施並維護一套全面性的安全計畫，以：

1. 保護憑證資料（Certificate Data）與憑證管理流程（Certificate Management Processes）之機密性、完整性及可用性；
2. 防範對憑證資料與憑證管理流程之機密性、完整性及可用性構成預期威脅或危害的情形；
3. 防範任何憑證資料或憑證管理流程遭未經授權或非法之存取、使用、揭露、變更或破壞；
4. 防範任何憑證資料或憑證管理流程遭意外遺失、毀損或損害；以及
5. 遵循法律對 CA 所適用之其他所有安全要求。

憑證管理流程**應（MUST）**包括：

1. 實體安全與環境控制；
2. 系統完整性控管，包括組態管理、受信任程式碼之完整性維護，以及惡意軟體之偵測與防範；
3. 網路安全與防火牆管理，包括連接埠限制及 IP 位址過濾；
4. 使用者管理、信賴角色（Trusted Role）之職責分離、教育、認知及訓練；以及
5. 邏輯存取控制、活動記錄及閒置逾時機制，以確保個別責任歸屬。

CA 的安全計畫**應（MUST）**包括每年執行之風險評估（Risk Assessment），該風險評估應：

1. 識別可預見的內部及外部威脅，該等威脅可能導致任何憑證資料或憑證管理流程遭未經授權之存取、揭露、誤用、變更或破壞；

2. 考量憑證資料與憑證管理流程之敏感性，評估該等威脅發生之可能性及其潛在損害；以及

3. 評估 CA 為了因應該等威脅所建立之政策、程序、資訊系統、技術及其他措施是否足以因應該等威脅。

基於風險評估結果，CA **應（SHALL）**建立、實施並維護一套安全計畫，該安全計畫應由安全程序、措施及產品組成，其目的在於達成前述目標，並依據憑證資料及憑證管理流程之敏感性，管理及控管風險評估中所識別之風險。該安全計畫**應（MUST）**包括與憑證資料及憑證管理流程之敏感性相應的行政、組織、技術及實體保護措施。該安全計畫亦**應（MUST）**考量當時可取得之技術，以及實施具體措施所需之成本，並**應（SHALL）**採行與安全事件所造成的潛在損害與受保護資料性質相應之合理安全水準。

# 5.1 實體安全控管

## 5.1.1 場址與建築構造

## 5.1.2 實體存取

## 5.1.3 電力與空調

## 5.1.4 觸水防範

## 5.1.5 火災預防與防護

## 5.1.6 媒體儲存

## 5.1.7 廢棄物處置

## 5.1.8 異地備援

# 5.2 作業程序控管

## 5.2.1 信賴角色

## 5.2.2 每項任務所需之人數

憑證機構私密金鑰（CA Private Key）**應（SHALL）**僅得由信賴角色（Trusted Role）之人員，於實體安全環境下，採用至少雙人的控管機制，以進行備份、儲存及復原。

### 5.2.3 每種角色之識別與鑑別

### 5.2.4 需要職責分離之角色

## 5.3 人員控管

### 5.3.1 適任條件、經歷及安全評估之要求

任何人在開始參與憑證管理流程（Certificate Management Process）之前，無論其身分為憑證機構（Certification Authority，CA）之員工、代理人或獨立承攬人，CA **應（SHALL）**驗證其身分及可信度。

### 5.3.2 背景調查程序

### 5.3.3 教育訓練要求與程序

憑證機構（Certification Authority，CA）**應（SHALL）**對所有執行資訊驗證職責之人員提供技能訓練，其內容應涵蓋基本公開金鑰基礎建設（Public Key Infrastructure，PKI）知識、鑑別與審查之政策及程序（包括 CA 的憑證政策（Certificate Policy，CP）及／或憑證實務作業基準（Certification Practice Statement，CPS））、資訊驗證流程中的常見威脅（包括網路釣魚及其他社交工程手法），以及本文件要求規定。

CA **應（SHALL）**保存此類教育訓練之記錄，並確保受委任執行驗證專員（Validation Specialist）職責之人員，維持足以妥善履行該等職責之技能水準。

CA **應（SHALL）**於允許驗證專員執行任務前，留存文件證明驗證專員均已具備執行該任務所需之技能。

CA **應（SHALL）**要求所有驗證專員通過由 CA 辦理、內容涵蓋本文件所列資訊驗證要求之測驗。

### 5.3.4 複訓頻率與要求

所有擔任信賴角色（Trusted Role）之人員**應（SHALL）**維持符合憑證機構（Certification Authority，CA）教育訓練及績效管理制度所要求之技能水準。

### 5.3.5 職務輪調之頻率與順序

### 5.3.6 未經授權行為之懲處

### 5.3.7 獨立承攬人之控管

憑證機構（Certification Authority，CA）**應（SHALL）**驗證受委任第三方（Delegated Third Party）參與憑證簽發之人員，是否符合第 5.3.3 節之教育訓練及技能要求，以及第 5.4.1 節之文件保留與事件記錄要求。

### 5.3.8 提供給人員之文件

## 5.4 稽核紀錄程序

### 5.4.1 應記錄之事件類型

憑證機構（Certification Authority，CA）及每個受委任第三方（Delegated Third Party）**應（SHALL）**記錄其憑證系統（Certificate System）、憑證管理系統（Certificate Management System）、根憑證機構系統（Root CA System）及受委任第三方系統（Delegated Third Party Systems）之安全有關的事件。CA 及每個受委任第三方**應（SHALL）**記錄其處理憑證申請及簽發憑證所採取之措施，包括與該憑證申請相關而產生之所有資訊、所接收之文件、處理之時間與日期，以及參與之人員。CA **應（SHALL）**提供此類紀錄供其合格稽核業者（Qualified Auditor）查核，作為 CA 遵循本文件要求規定之證明。

CA **應（SHALL）**至少記錄下列事件：

1. CA 憑證及金鑰生命週期事件，包括：
    1. 金鑰之產生、備份、儲存、復原、封存及銷毀；
    2. 憑證申請、憑證展期與金鑰更換請求，以及廢止；
    3. 憑證申請之核准與拒絕；
    4. 密碼學裝置（Cryptographic Device）生命週期管理事件；
    5. 憑證廢止清冊（Certificate Revocation List，CRL）之產生；
    6. OCSP 回應之簽章（如第 4.9 節及第 4.10 節所述）；以及
    7. 新增憑證剖繪（Certificate Profiles）及現有憑證剖繪之退役。
2. 用戶憑證（Subscriber Certificate）生命週期管理事件，包括：
    1. 憑證申請、憑證展期與金鑰更換請求，以及廢止；
    2. 本文件及 CA 憑證實務作業基準（Certification Practice Statement，CPS）所規定之所有驗證活動。自 2026-07-15 起，紀錄**應（MUST）**至少包含：
        1. 受驗證之資訊（例如所申請的完全吻合網域名稱（FQDN）或組織名稱）；
        2. 所使用之經授權網域名稱（ADN）（若適用，且所使用之經授權網域名稱（ADN）與所申請的 FQDN 不相同）；以及

3. 所使用之驗證方法（例如《基本要求》的章節編號或 ACME 驗證方法於 IANA 登記之名稱（registered label））；

3. 憑證申請之核准與拒絕；
4. 憑證之簽發；
5. 憑證廢止清冊（CRL）之產生；以及
6. OCSP 回應之簽章（如第 4.9 節及第 4.10 節所述）。
7. 每個網路視角（Network Perspective）執行多視角簽發佐證（Multi-Perspective Issuance Corroboration）時，至少應記錄下列資訊：
   1. 用以識別所使用之網路視角的唯一識別碼；
   2. 進行驗證之網域名稱及／或 IP 位址；以及
   3. 該次執行之結果（例如「網域驗證通過／失敗」、「CAA 許可／禁止」）。
8. 憑證申請所包含之每個網域名稱或 IP 位址的多視角簽發佐證法定數量（Quorum）結果（例如「3/4」，表示 4 個網路視角中，有 3 個佐證了主要網路視角（Primary Network Perspective）所做之判定」）。

3. 安全事件，包括：
   1. PKI（公開金鑰基礎建設）系統存取成功及失敗之結果；
   2. PKI 及安全系統所執行之操作；
   3. 安全剖繪（Security profile）變更；
   4. 憑證系統（Certificate System）上之軟體安裝、更新及移除；
   5. 系統當機、硬體故障及其他異常；
   6. 相關路由器及防火牆活動（如第 5.4.1.1 節所述）；以及
   7. 進出 CA 設施之記錄。

紀錄內容**應（MUST）**至少包含下列要素：

1. 事件發生日期與時間；
2. 建立該事件紀錄之人員識別資訊（若適用）；以及
3. 事件內容描述。

#### 5.4.1.1 路由器與防火牆活動紀錄

為了符合第 5.4.1 節第 3.6 項之要求，路由器及防火牆活動之記錄**應（MUST）**至少包含：

1. 路由器及防火牆的成功與失敗之登入結果；以及
2. 對路由器與防火牆執行之所有管理操作的記錄，包括組態變更、韌體更新及存取控制修改；以及

3. 防火牆規則之所有變更記錄，包括新增、修改及刪除；以及
4. 所有系統事件與錯誤之記錄，包括硬體故障、軟體異常終止及系統重新啟動。

### 5.4.2 稽核紀錄處理頻率

### 5.4.3 稽核紀錄之保留期限

憑證機構（Certification Authority，CA）及每個受委任第三方（Delegated Third Party）**應（SHALL）**將下列資料至少保留 2 年：

1. CA 憑證及金鑰生命週期管理事件紀錄（如第 5.4.1 節第（1）項所規定），自下列事項中較晚發生者為起算點：
    1. CA 私密金鑰遭銷毀；或
    2. 具有 X.509v3 `basicConstraints` 擴充欄位（其 `cA` 欄位設為 TRUE），且共用該 CA 私密金鑰所對應之同一把公開金鑰的憑證集合中，最後一張 CA 憑證遭廢止或到期；
2. 用戶憑證生命週期管理事件紀錄（如第 5.4.1 節第（2）項所規定），以用戶憑證到期為起算點；
3. 安全事件紀錄（如第 5.4.1 節第（3）項所規定），以事件發生為起算點。

**注意**：本文件僅規定最低保留期限，CA **得（MAY）**視需求選擇較長之保留期限，以利日後調查可能發生、需回溯檢視過往稽核紀錄之安全事故或其他類型事故。

### 5.4.4 稽核紀錄之保護

### 5.4.5 稽核紀錄備份程序

### 5.4.6 稽核紀錄彙整系統（內部或外部）

### 5.4.7 對引發事件者之通知

### 5.4.8 弱點評估

此外，憑證機構（Certification Authority，CA）的安全計畫**應（MUST）**包括每年執行之風險評估，該風險評估應：

1. 識別可預見之內部與外部威脅，該等威脅可能導致任何憑證資料（Certificate Data）及憑證管理流程（Certificate Management Processes）發生未經授權之存取、揭露、誤用、變更或破壞；
2. 考量憑證資料及憑證管理流程的敏感性，評估該等威脅之發生可能性與潛在損害；以及

3. 評估 CA 為了因應該等威脅所建立之政策、程序、資訊系統、技術及其他安排措施是否足夠。

## 5.5 紀錄歸檔

### 5.5.1 歸檔紀錄之類型

憑證機構（Certification Authority，CA）及每個受委任第三方（Delegated Third Party）**應（SHALL）**歸檔所有稽核紀錄（如第 5.4.1 節所規定）。

此外，CA 及每個受委任第三方**應（SHALL）**歸檔下列資料：

1. 與其憑證系統（Certificate System）、憑證管理系統（Certificate Management Systems）、根憑證機構系統（Root CA Systems）及受委任第三方系統（Delegated Third Party Systems）之安全有關的文件；以及

2. 與其對憑證申請及憑證所進行之驗證、簽發及廢止有關的文件。

### 5.5.2 歸檔紀錄之保留期限

歸檔之稽核紀錄（如第 5.5.1 節所規定）**應（SHALL）**自其紀錄建立時間戳記起保留至少 2 年，或按照第 5.4.3 節對此類紀錄所規定之保留期限，以較長者為準。

此外，憑證機構（Certification Authority，CA）及每個受委任第三方（Delegated Third Party）**應（SHALL）**將下列資料至少保留 2 年：

1. 所有已歸檔之與憑證系統（Certificate Systems）、憑證管理系統（Certificate Management Systems）、根憑證機構系統（Root CA Systems）及受委任第三方系統（Delegated Third Party Systems）之安全有關的文件（如第 5.5.1 節所規定）；以及

2. 所有與憑證申請及憑證所進行之驗證、簽發及廢止有關之已歸檔文件（如第 5.5.1 節所規定），自下列事項中較晚發生者起至少保留 2 年：

    1. 此類紀錄及文件最後一次作為憑證申請及憑證之驗證、簽發或廢止之依據；或

    2. 依據此類紀錄及文件簽發之用戶憑證到期。

**注意**：本文件僅規定最低保留期限，CA **得（MAY）**視需求選擇較長之保留期限，以利日後調查可能發生、需回溯檢視過往已歸檔紀錄之安全事故或其他類型事故。

### 5.5.3 歸檔紀錄之保護

### 5.5.4 歸檔紀錄備份程序

### 5.5.5 紀錄之時戳要求

### 5.5.6 歸檔紀錄彙整系統（內部或外部）

### 5.5.7 取得及驗證歸檔資訊之程序

## 5.6 憑證機構之金鑰交替

## 5.7 遭受危害及災變復原

### 5.7.1 事故及遭受危害之處理程序

#### 5.7.1.1 事故應變及災變復原計畫

各憑證機構應具備事故應變計畫及災變復原計畫。

憑證機構（Certification Authority，CA）**應（SHALL）**將業務持續性與災變復原程序作成文件，以便於發生災變、安全遭受危害或營運失敗時，通知並合理保護應用軟體供應商（Application Software Supplier）、用戶（Subscriber）及信賴憑證者（Relying Party）。CA 無須對外公開其業務持續性計畫，但**應（SHALL）**於其稽核人員要求時，提供其業務持續性計畫及安全計畫供查核。CA **應（SHALL）**每年測試、審查及更新該等程序。

業務持續性計畫（Business Continuity Plan）**應（MUST）**包括：

1. 計畫啟動條件，
2. 緊急程序，
3. 備援程序，
4. 營運恢復程序，
5. 計畫之維護時程；
6. 認知宣導及教育訓練要求；
7. 相關人員之職責；
8. 復原時間目標（Recovery Time Objective，RTO）；
9. 應變計畫的定期演練。
10. CA 於關鍵業務流程中斷或失敗後，於期限內維持或恢復其業務營運之計畫

11. 要求將關鍵密碼學材料（即安全密碼學裝置及啟動資料）存放於備用地點；

12. 可接受的系統停機及復原時間之定義

13. 基本業務資訊與軟體的備份頻率；

14. 復原設施與 CA 主要營運場地之間的距離；以及

15. 災變發生後，於原始場地或遠距場地恢復安全環境前，儘可能確保其設施安全之程序。

#### 5.7.1.2 大規模廢止計畫

各憑證機構**應（MUST）**具備大規模廢止計畫，且自 2025-12-01 起，**應（SHALL）**於其憑證實務作業基準（CPS）或合併式 CP/CPS 的第 5.7.1 節中聲明，其已建立並持續維護一套針對大規模廢止事件之完整且可執行的計畫，並每年對該大規模廢止計畫進行演練，將演練所得之經驗教訓回饋至該計畫，以持續提升其應對大規模廢止事件之整備能力。

憑證機構（Certification Authority，CA）的大規模廢止計畫**應（MUST）**包括明確界定、可執行且完整之程序，以確保大規模憑證廢止的情境下，能做出迅速、一致且可靠之回應。CA 無須對外公開其大規模廢止計畫或程序，但**應（MUST）**於其稽核人員要求時，提供該等計畫及程序供查核。CA **應（SHALL）**每年測試、審查及更新其計畫及該等程序。CA 的大規模廢止計畫**得（MAY）**整合至 CA 的事故應變計畫、業務持續性計畫、災變復原計畫或其他類似計畫或程序中，前提是大規模廢止事件之應變條款仍應清楚可識別，且符合本節要求規定。

大規模廢止事件應變條款**應（MUST）**包括：

1. 啟動要件——根據 CA 的風險剖繪（risk profile）、簽發量及營運能力，設定啟動大規模廢止計畫之具體、客觀且可衡量的門檻條件；

2. 客戶聯絡資訊——用戶與客戶的詳細聯絡資訊之儲存、維護及更新方式；

3. 自動化環節——已自動化或可自動化之流程，以及需人工介入之流程；

4. 目標與時程——事故研判（incident triage）、發起憑證廢止、憑證更換及事後審查之目標與時程；

5. 用戶通知方式——通知受影響用戶之機制；

6. 角色指派——負責發起、協調及執行大規模廢止計畫的人員之角色與職責；

7. 訓練與教育——大規模廢止計畫的負責人員或支援人員之訓練、認知及整備活動；

8. 計畫演練——每年進行一次實作演練，以評估整備能力並驗證實施可行性，採用下列一種或多種方式：桌上演練（tabletop exercises）、模擬演練、平行演練，或**不涉及**廢止有效用戶憑證之受控測試環境演練；以及

9. 演練後分析與更新時程——如何將演練或實際發生事故所得之經驗教訓回饋至計畫，以及計畫的審查與更新頻率。

### 5.7.2 運算資源、軟體及／或資料遭損毀時之復原程序

### 5.7.3 憑證機構金鑰遭破解之處理程序

### 5.7.4 災變後之業務持續能力

## 5.8 憑證機構或註冊中心終止服務

---

# 6 技術安全控管

## 6.1 金鑰對產製與安裝

### 6.1.1 金鑰對之產製

#### 6.1.1.1 憑證機構（CA）金鑰對之產製

對於符合下列任一情形之憑證機構（CA）金鑰對：

i. 作為根憑證（Root Certificate）之 CA 金鑰對使用；或

ii. 作為下屬憑證機構憑證（Subordinate CA Certificate）之 CA 金鑰對使用，且該下屬憑證機構（Subordinate CA）並非根憑證機構（Root CA）之營運者，亦非根憑證機構之關係企業（Affiliate），

憑證機構（Certification Authority，CA）**應（SHALL）**：

1. 準備並遵從金鑰產製腳本（Key Generation Script），
2. 由合格稽核業者（Qualified Auditor）見證 CA 金鑰對之產製流程，或錄製整個 CA 金鑰對產製流程之影片，以及
3. 由合格稽核業者出具報告，就下列事項表示意見：CA 於其金鑰及憑證產製流程中已遵從其金鑰儀式（Key Ceremony），以及用於確保該金鑰對完整性與機密性之控管措施已妥善實施。

對於供根憑證機構（Root CA）營運者或根憑證機構關係企業使用之其他 CA 金鑰對，憑證機構（CA）**宜（SHOULD）**：

1. 準備並遵從金鑰產製腳本，以及

2. 由合格稽核業者見證 CA 金鑰對之產製流程，或錄製整個 CA 金鑰對產製流程之影片。

在所有情況下，憑證機構（CA）**應（SHALL）**：

1. 依據 CA 的憑證政策（Certificate Policy，CP）及／或憑證實務作業基準（Certification Practice Statement，CPS）所述，於實體安全環境中產製 CA 金鑰對；
2. 由擔任信賴角色（Trusted Role）之人員，依循多人控管（multiple person control）及分拆知識（split knowledge）原則產製 CA 金鑰對；
3. 於符合 CA 憑證政策（CP）及／或憑證實務作業基準（CPS）所載之適用技術及業務要求規定的密碼模組（cryptographic module）內產製 CA 金鑰對；
4. 記錄其 CA 金鑰對產製活動；以及
5. 維持有效的控管措施，以便合理確信私密金鑰係依其憑證政策（CP）及／或憑證實務作業基準（CPS）所述之程序，以及（若適用）其金鑰產製腳本產製而成並受到保護。

#### 6.1.1.2 註冊中心（RA）金鑰對之產製

#### 6.1.1.3 用戶金鑰對之產製

若符合下列一項或多項條件，憑證機構（Certification Authority，CA）**應（SHALL）**拒絕憑證申請：

1. 金鑰對不符合第 6.1.5 節及／或第 6.1.6 節所定之要求；
2. 有明確證據顯示，用於產製該私密金鑰之特定方法存在缺陷；
3. CA 獲悉已有經展示或證實之方法，足以使申請者之私密金鑰遭受破解（compromise）；
4. CA 先前已接獲依據第 4.9.3 節及第 4.9.12 節所述之 CA 憑證廢止請求程序所提出之通知，指出申請者之私密金鑰已發生金鑰遭破解（Key Compromise）；
5. 公開金鑰（Public Key）所對應之私密金鑰（Private Key），經業界證實屬弱金鑰。至少**應（SHALL）**實施下列預防措施：
    1. 針對 Debian 弱金鑰（Debian weak keys）漏洞（https://wiki.debian.org/SSLkeys），CA **應（SHALL）**拒絕 https://github.com/cabforum/Debian-weak-keys/ 儲存庫中針對各金鑰類型（例如 RSA、ECDSA）及金鑰長度所列之所有弱金鑰。對於其他符合第 6.1.5 節要求之所有金鑰（RSA 金鑰長度超過 8192 位元者除外），CA **應（SHALL）**拒絕符合 Debian 弱金鑰漏洞之金鑰。
    2. 針對 ROCA 漏洞，CA **應（SHALL）**拒絕經 https://github.com/crocs-muni/roca 所提供之工具或其他具同等功能工具檢測，識別為受 ROCA 漏洞影響之金鑰。
    3. 針對接近質數漏洞（Close Primes vulnerability）（https://fermatattack.secvuln.info/），CA **應（SHALL）**拒絕可於費馬因式分解法（Fermat’s factorization method）重複 100 次步驟內完成因式分解之弱金鑰。

可用於檢查弱金鑰之建議工具請參閱：https://cabforum.org/resources/tools/

若用戶憑證（Subscriber Certificate）將包含 `extKeyUsage` 擴充欄位，且其中包含 `id-kp-serverAuth`（RFC 5280）或 `anyExtendedKeyUsage`（RFC 5280）值，CA **不得（SHALL NOT）**代表用戶產製金鑰對，亦**不得（SHALL NOT）**接受以 CA 先前產製之金鑰對所提出的憑證申請。

### 6.1.2 私密金鑰交付予用戶

用戶（Subscriber）以外之任何一方，未經用戶授權，**不得（SHALL NOT）**保留（archive）用戶之私密金鑰。

若憑證機構（Certification Authority，CA）或其任何指定之註冊中心（Registration Authority，RA）獲悉用戶之私密金鑰已提供予未經授權之人員，或提供予與用戶無關聯之組織，則 CA **應（SHALL）**廢止所有包含與該已提供私密金鑰相對應之公開金鑰的憑證。

### 6.1.3 用戶之公開金鑰交付予憑證簽發者

### 6.1.4 憑證機構（CA）之公開金鑰交付予信賴憑證者

### 6.1.5 金鑰長度

對於 RSA 金鑰對，憑證機構（Certification Authority，CA）**應（SHALL）**：

- 確保模數（modulus）經編碼後，長度至少為 2048 位元；且
- 確保模數長度（以位元計）為 8 的整數倍。

對於 ECDSA 金鑰對，CA **應（SHALL）**：

- 確保該金鑰所表示之點，係 NIST P-256、NIST P-384 或 NIST P-521 橢圓曲線上的有效點。

不得使用其他演算法或金鑰長度。

### 6.1.6 公開金鑰參數之產製與品質檢查

RSA：憑證機構（Certification Authority，CA）**應（SHALL）**確認公開指數（public exponent）之值為大於或等於 3 的奇數。此外，公開指數**宜（SHOULD）**介於 2^16 + 1 與 2^256 - 1 之間。模數亦**宜（SHOULD）**具有下列特性：為奇數、非任何質數的冪，且不具有小於 752 的因數。〔來源：NIST SP 800-89 第 5.3.3 節〕

ECDSA：CA **宜（SHOULD）**使用 ECC 完整公開金鑰驗證程序（ECC Full Public Key Validation Routine）或 ECC 部分公開金鑰驗證程序（ECC Partial Public Key Validation Routine），確認所有金鑰的有效性。〔來源：NIST SP 800-56A：修訂第 2 版 第 5.6.2.3.2 節及第 5.6.2.3.3 節〕

### 6.1.7 憑證金鑰用途（比照 X.509 v3 `keyUsage` 欄位）

對應至根憑證（Root Certificate）的私密金鑰，**不得（MUST NOT）**用於簽章下列以外之任何憑證：

1. 代表根憑證機構（Root CA）本身之自簽憑證；
2. 下屬憑證機構憑證（Subordinate CA Certificate）與交互認證之下屬憑證機構憑證（Cross-Certified Subordinate CA Certificate）；
3. 供基礎設施用途之憑證（例如行政角色憑證、CA 內部營運裝置憑證）；以及
4. 用於驗證 OCSP 回應之憑證。

## 6.2 私密金鑰保護及密碼模組工程控管

憑證機構（Certification Authority，CA）**應（SHALL）**實施實體及邏輯保護措施，以防止未經授權之憑證簽發。位於第 6.2.7 節指定之已驗證系統或裝置以外的 CA 私密金鑰，其保護措施**應（MUST）**採用實體安全、加密，或兩者之組合，且其實施方式須能防止私密金鑰遭揭露。CA **應（SHALL）**使用依據當前技術水準，足以在加密金鑰或金鑰部分之剩餘有效期內抵抗密碼分析攻擊的演算法及金鑰長度，加密其私密金鑰。

### 6.2.1 密碼模組標準與控管

### 6.2.2 私密金鑰（n／m）多人控管

### 6.2.3 私密金鑰託管

### 6.2.4 私密金鑰備份

參見第 5.2.2 節。

### 6.2.5 私密金鑰歸檔

下屬憑證機構（Subordinate CA）以外之任何一方，未經下屬憑證機構授權，**不得（SHALL NOT）**歸檔保留下屬憑證機構之私密金鑰。

### 6.2.6 私密金鑰匯入密碼模組或自密碼模組匯出

若簽發憑證機構（Issuing CA）代表下屬憑證機構（Subordinate CA）產製私密金鑰，則簽發憑證機構**應（SHALL）**為了將其傳送至下屬憑證機構，而加密該私密金鑰。若簽發憑證機構獲悉下屬憑證機構之私密金鑰已提供予未經授權之人員，或提供予與下屬憑證機構無關聯之組織，則簽發憑證機構**應（SHALL）**廢止所有包含與該已提供私密金鑰相對應之公開金鑰的憑證。

### 6.2.7 私密金鑰儲存於密碼模組

憑證機構（Certification Authority，CA）**應（SHALL）**於經驗證至少符合下列任一標準之系統或裝置中保護其私密金鑰：FIPS 140-2 Level 3、FIPS 140-3 Level 3，或達到 EAL 4（或更高等級）之適當 Common Criteria Protection Profile 或 Security Target 標準，上述標準應包含保護私密金鑰及其他資產免於已知威脅之要求。

### 6.2.8 啟動私密金鑰之方式

### 6.2.9 停用私密金鑰之方式

### 6.2.10 銷毀私密金鑰之方式

### 6.2.11 密碼模組等級

## 6.3 金鑰對管理之其他事項

### 6.3.1 公開金鑰歸檔

### 6.3.2 憑證效期與金鑰對使用期間

於 2026-03-15 前簽發之用戶憑證（Subscriber Certificate），其有效期限（Validity Period）**不宜（SHOULD NOT）**超過 397 日，且**不得（MUST NOT）**超過 398 日。

於 2026-03-15 當日或之後、2027-03-15 前簽發之用戶憑證，其有效期限**不宜（SHOULD NOT）**超過 199 日，且**不得（MUST NOT）**超過 200 日。

於 2027-03-15 當日或之後、2029-03-15 前簽發之用戶憑證，其有效期限**不宜（SHOULD NOT）**超過 99 日，且**不得（MUST NOT）**超過 100 日。

於 2029-03-15 當日或之後簽發之用戶憑證，其有效期限**不宜（SHOULD NOT）**超過 46 日，且**不得（MUST NOT）**超過 47 日。

| 憑證於此日或之後簽發 | 憑證於此日前簽發 | 憑證有效期之最長期限 |
| --- | --- | --- |
| | 2026-03-15 | 398 日 |
| 2026-03-15 | 2027-03-15 | 200 日 |
| 2027-03-15 | 2029-03-15 | 100 日 |
| 2029-03-15 | | 47 日 |

用戶憑證最長有效期限之參考表格

計算時，1 日以 86,400 秒計。任何超出此時間之時間長度，包括不足 1 秒及／或閏秒，均視為額外的 1 日。因此，為因應此類調整，用戶憑證**不宜（SHOULD NOT）**預設以規定所允許之最大天數簽發。

## 6.4 啟動資料

### 6.4.1 啟動資料之產製與安裝

### 6.4.2 啟動資料之保護

### 6.4.3 啟動資料之其他事項

## 6.5 電腦安全控管

### 6.5.1 電腦安全之具體技術要求

憑證機構（Certification Authority，CA）**應（SHALL）**對所有可直接執行憑證簽發作業之帳號，強制執行多因子驗證（multi-factor authentication）。

### 6.5.2 電腦安全等級

## 6.6 系統生命週期之技術控管

### 6.6.1 系統開發控管

若憑證機構（Certification Authority，CA）使用第三方開發的 Linting 軟體，**宜（SHOULD）**留意該軟體是否發布更新版本，並規劃於更新版本發布後 3 個月內完成更新。

CA **得（MAY）**於每次更新 Linting 軟體時，對其所有未到期且未廢止之用戶憑證執行 Linting。

### 6.6.2 安全管理控管

### 6.6.3 系統生命週期安全控管

## 6.7 網路安全控管

## 6.8 時間戳記

---

# 7 憑證、憑證廢止清冊（CRL）與線上憑證狀態協定（OCSP）剖繪

## 7.1 憑證剖繪

憑證機構（Certification Authority，CA）**應（SHALL）**符合第 6.1.5 節（金鑰長度）及第 6.1.6 節（公開金鑰參數之產製與品質檢查）所規定之技術要求。

CA **應（SHALL）**依本文件所規定之剖繪（profile）簽發憑證。

### 7.1.1 版本號

憑證**應（MUST）**採用 X.509 v3 版本。

### 7.1.2 憑證內容與擴充欄位

若憑證機構（Certification Authority，CA）聲明其遵循本《基本要求》規定，則其所簽發之所有憑證**應（MUST）**遵循下列其中一種憑證剖繪（Certificate Profiles）；該等憑證剖繪引用 RFC 5280 之相關規定，並以其為基礎衍生。除非另有明確說明，除本文件所規定之規範性要求外，RFC 5280 所定之所有規範性要求亦適用。CA **宜（SHOULD）**參閱 RFC 5280 附錄 B，以瞭解其他應注意事項。

- 憑證機構（CA）憑證
  - 第 7.1.2.1 節－根憑證機構（Root CA）憑證剖繪
  - 下屬憑證機構憑證（Subordinate CA Certificates）
    - 交互憑證（Cross Certificates）
      - 第 7.1.2.2 節－交互認證之下屬憑證機構（Cross-Certified Subordinate CA）憑證剖繪

    - 受技術約束之憑證機構憑證（Technically Constrained CA Certificates）
        - 第 7.1.2.3 節－受技術約束之非 TLS 下屬憑證機構（Technically-Constrained Non-TLS Subordinate CA）憑證剖繪
        - 第 7.1.2.4 節－受技術約束之預簽憑證簽章憑證機構（Technically-Constrained Precertificate Signing CA）憑證剖繪
        - 第 7.1.2.5 節－受技術約束之 TLS 下屬憑證機構（Technically-Constrained TLS Subordinate CA）憑證剖繪
    - 第 7.1.2.6 節－TLS 下屬憑證機構（TLS Subordinate CA）憑證剖繪
- 第 7.1.2.7 節－用戶（終端個體）（Subscriber (End-Entity)）憑證剖繪
- 第 7.1.2.8 節－OCSP 回應伺服器（OCSP Responder）憑證剖繪
- 第 7.1.2.9 節－預簽憑證（Precertificate）剖繪

### 7.1.2.1 根憑證機構（Root CA）憑證剖繪

| 欄位 | 說明 |
| --- | --- |
| `tbsCertificate` | |
| `version` | **應（MUST）**為 v3(2) |
| `serialNumber` | **應（MUST）**為一個非連續之數值，其值大於 0 且小於 $2^{159}$，且其中至少 64 個位元應來自 CSPRNG 之輸出。 |
| `signature` | 參見第 7.1.3.2 節 |
| `issuer` | 編碼後之值**應（MUST）**與編碼後的 `subject` 逐位元組完全相同。 |
| `validity` | 參見第 7.1.2.1.1 節 |
| `subject` | 參見第 7.1.2.10.2 節 |
| `subjectPublicKeyInfo` | 參見第 7.1.3.1 節 |
| `issuerUniqueID` | **不得（MUST NOT）**存在 |
| `subjectUniqueID` | **不得（MUST NOT）**存在 |
| `extensions` | 參見第 7.1.2.1.2 節 |
| `signatureAlgorithm` | 編碼後之值**應（MUST）**與 `tbsCertificate.signature` 逐位元組完全相同 |
| `signature` | |

#### 7.1.2.1.1 根憑證機構（Root CA）之有效期

| 欄位 | 最小值 | 最大值 |
| --- | --- | --- |
| `notBefore` | 簽章時間前 1 日 | 簽章時間 |
| `notAfter` | 2922 日（約 8 年） | 9132 日（約 25 年） |

**注意**：即使使用既有的 `subject` 與 `subjectPublicKeyInfo` 產生新的根憑證機構（Root CA）憑證（例如重新簽發），上述限制仍適用。新的 CA 憑證**應（MUST）**符合這些規定。

#### 7.1.2.1.2 根憑證機構（Root CA）之擴充欄位

| 擴充欄位 | 必要性 | 關鍵性 | 說明 |
| --- | --- | --- | --- |
| `authorityKeyIdentifier` | 建議（RECOMMENDED） | N | 參見第 7.1.2.1.3 節 |
| `basicConstraints` | 應（MUST） | Y | 參見第 7.1.2.1.4 節 |
| `keyUsage` | 應（MUST） | Y | 參見第 7.1.2.10.7 節 |
| `subjectKeyIdentifier` | 應（MUST） | N | 參見第 7.1.2.11.4 節 |
| `extKeyUsage` | 不得（MUST NOT） | - | - |
| `certificatePolicies` | 不建議（NOT RECOMMENDED） | N | 參見第 7.1.2.10.5 節 |
| Signed Certificate Timestamp（SCT）清單 | 得（MAY） | N | 參見第 7.1.2.11.3 節 |
| 任何其他擴充欄位 | 不建議（NOT RECOMMENDED） | - | 參見第 7.1.2.11.5 節 |

#### 7.1.2.1.3 根憑證機構（Root CA）之授權單位金鑰識別碼（Authority Key Identifier）

| 欄位 | 說明 |
| --- | --- |
| `keyIdentifier` | **應（MUST）**存在。**應（MUST）**與 `subjectKeyIdentifier` 欄位完全相同。 |
| `authorityCertIssuer` | **不得（MUST NOT）**存在 |
| `authorityCertSerialNumber` | **不得（MUST NOT）**存在 |

#### 7.1.2.1.4 根憑證機構（Root CA）之基本限制（Basic Constraints）

| 欄位 | 說明 |
| --- | --- |
| `cA` | **應（MUST）**設為 TRUE |
| `pathLenConstraint` | 不建議（NOT RECOMMENDED） |

### 7.1.2.2 交互認證之下屬憑證機構（Cross-Certified Subordinate CA）憑證剖繪

當簽發之 CA 憑證與一張或多張現有 CA 憑證（無論為根憑證機構（Root CA）憑證或下屬憑證機構（Subordinate CA）憑證）具有相同之主體名稱（Subject Name）及主體公開金鑰資訊（Subject Public Key Information）時，**得（MAY）**使用本憑證剖繪。

於簽發交互認證之下屬憑證機構（Cross-Certified Subordinate CA）憑證前，簽發憑證機構（Issuing CA）**應（MUST）**確認一張或多張既有 CA 憑證受本《基本要求》規範，且於簽發時係遵循當時有效版本之《基本要求》所簽發。

| 欄位 | 說明 |
| --- | --- |
| `tbsCertificate` | |
| `version` | **應（MUST）**為 v3(2) |
| `serialNumber` | **應（MUST）**為一個非連續之數值，其值大於 0 且小於 $2^{159}$，且其中至少 64 個位元應來自 CSPRNG 之輸出。 |
| `signature` | 參見第 7.1.3.2 節 |
| `issuer` | **應（MUST）**與簽發憑證機構（Issuing CA）之 `subject` 欄位逐位元組完全相同。參見第 7.1.4.1 節 |
| `validity` | 參見第 7.1.2.2.1 節 |
| `subject` | 參見第 7.1.2.2.2 節 |
| `subjectPublicKeyInfo` | 參見第 7.1.3.1 節 |
| `issuerUniqueID` | **不得（MUST NOT）**存在 |
| `subjectUniqueID` | **不得（MUST NOT）**存在 |
| `extensions` | 參見第 7.1.2.2.3 節 |
| `signatureAlgorithm` | 編碼後之值**應（MUST）**與 `tbsCertificate.signature` 逐位元組完全相同 |
| `signature` | |

#### 7.1.2.2.1 交互認證之下屬憑證機構（Cross-Certified Subordinate CA）之有效期

| 欄位 | 最小值 | 最大值 |
| --- | --- | --- |
| `notBefore` | 簽章時間前 1 日或既有 CA 憑證之最早 `notBefore` 日期，兩者取較早者。 | 簽章時間 |
| `notAfter` | 簽章時間 | 未指定 |

#### 7.1.2.2.2 交互認證之下屬憑證機構（Cross-Certified Subordinate CA）之填名（Naming）

`subject` **應（MUST）**遵循第 7.1.4 節之要求；或者，若既有 CA 憑證係遵循當時有效版本之《基本要求》所簽發，則編碼後的 `subject` 名稱**應（MUST）**與既有 CA 憑證之編碼後的 `subject` 名稱逐位元組完全相同。

**注意**：上述「編碼後逐位元組完全相同」之例外，允許 CA 在既有 CA 憑證遵循其簽發當時有效之《基本要求》的前提下，簽發交互認證之下屬憑證機構（Cross-Certified Subordinate CA）憑證。此例外使第 7.1.4 節之要求得以隨時間持續改進，同時仍允許進行交互認證。若既有 CA 憑證不遵循其簽發當時有效之《基本要求》，則不得簽發交互憑證。

#### 7.1.2.2.3 交互認證之下屬憑證機構（Cross-Certified Subordinate CA）之擴充欄位

| 擴充欄位 | 必要性 | 關鍵性 | 說明 |
| --- | --- | --- | --- |
| `authorityKeyIdentifier` | 應（MUST） | N | 參見第 7.1.2.11.1 節 |
| `basicConstraints` | 應（MUST） | Y | 參見第 7.1.2.10.4 節 |
| `certificatePolicies` | 應（MUST） | N | 參見第 7.1.2.2.6 節 |
| `crlDistributionPoints` | 應（MUST） | N | 參見第 7.1.2.11.2 節 |
| `keyUsage` | 應（MUST） | Y | 參見第 7.1.2.10.7 節 |
| `subjectKeyIdentifier` | 應（MUST） | N | 參見第 7.1.2.11.4 節 |
| `authorityInformationAccess` | 宜（SHOULD） | N | 參見第 7.1.2.10.3 節 |
| `nameConstraints` | 得（MAY） | *[1] | 參見第 7.1.2.10.8 節 |
| Signed Certificate Timestamp（SCT）清單 | 得（MAY） | N | 參見第 7.1.2.11.3 節 |
| 任何其他擴充欄位 | 不建議（NOT RECOMMENDED） | - | 參見第 7.1.2.11.5 節 |

除上述規定外，`extKeyUsage` 擴充欄位之要求，視交互憑證的簽發者與主體組織的關係而異。

若符合以下條件，`extKeyUsage` 擴充欄位**得（MAY）**依下表所述設為「不受限制」：

- 交互憑證的簽發者與主體名稱中的 `organizationName` 符合下列任一情形：

- 兩者相同，或
- 主體名稱中的 `organizationName` 為簽發者名稱中的 `organizationName` 之關係企業

- 交互憑證之主體 CA，係由簽發憑證機構（Issuing CA）所屬組織或其關係企業負責營運。

| 擴充欄位 | 必要性 | 關鍵性 | 說明 |
| --- | --- | --- | --- |
| `extKeyUsage` | 宜（SHOULD）[2] | N | 參見第 7.1.2.2.4 節 |

`extKeyUsage`（EKU）不受限制之交互認證之下屬憑證機構

在所有其他情況下，`extKeyUsage` 擴充欄位**應（MUST）**依下表所述設為「受限制」：

| 擴充欄位 | 必要性 | 關鍵性 | 說明 |
| --- | --- | --- | --- |
| `extKeyUsage` | 應（MUST）[2] | N | 參見第 7.1.2.2.5 節 |

`extKeyUsage`（EKU）受限制之交互認證之下屬憑證機構

### 7.1.2.2.4 交互認證之下屬憑證機構（Cross-Certified Subordinate CA）之擴充金鑰使用方法（Extended Key Usage）－不受限制（Unrestricted）

| 金鑰適用目的（Key Purpose） | 說明 |
| --- | --- |
| `anyExtendedKeyUsage` | 表示不受任何限制之特殊擴充金鑰使用方法。若存在，**應（MUST）**為唯一的擴充金鑰使用方法。 |
| 任何其他值 | 若存在 `anyExtendedKeyUsage` 擴充金鑰使用方法，CA **不得（MUST NOT）**包含任何其他擴充金鑰使用方法。 |

不受限制之擴充金鑰使用方法之適用目的（適用於關係企業之交互認證 CA）

或者，若簽發憑證機構（Issuing CA）不採用此形式，且 `extKeyUsage` 擴充欄位若存在，**應（MUST）**依第 7.1.2.2.5 節所規定之方式編碼。

### 7.1.2.2.5 交互認證之下屬憑證機構（Cross-Certified Subordinate CA）之擴充金鑰使用方法（Extended Key Usage）－受限制（Restricted）

受限制 TLS 交互認證之下屬憑證機構（Restricted TLS Cross-Certified Subordinate CA）之擴充金鑰使用方法適用目的（即適用於直接或間接簽發 TLS 憑證的受限制交互認證之下屬憑證機構）。

| 金鑰適用目的（Key Purpose） | 說明 |
| --- | --- |
| `id-kp-serverAuth` | **應（MUST）**存在 |
| `id-kp-clientAuth` | **得（MAY）**存在 |
| `id-kp-emailProtection` | **不得（MUST NOT）**存在 |
| `id-kp-codeSigning` | **不得（MUST NOT）**存在 |
| `id-kp-timeStamping` | **不得（MUST NOT）**存在 |
| `anyExtendedKeyUsage` | **不得（MUST NOT）**存在 |
| 任何其他值 | 不建議（NOT RECOMMENDED） |

TLS 交互認證之下屬憑證機構 `extKeyUsage`（EKU）

受限制非 TLS 交互認證之下屬憑證機構（Restricted Non-TLS Cross-Certified Subordinate CA）之擴充金鑰使用方法適用目的（即適用於不直接或不間接簽發 TLS 憑證的受限制交互認證之下屬憑證機構）。

| 金鑰適用目的（Key Purpose） | 說明 |
| --- | --- |
| `id-kp-serverAuth` | **不得（MUST NOT）**存在 |
| `anyExtendedKeyUsage` | **不得（MUST NOT）**存在 |
| 任何其他值 | **得（MAY）**存在 |

非 TLS 交互認證之下屬憑證機構 `extKeyUsage`（EKU）

每項被包含的擴充金鑰使用方法之適用目的：

1. **應（MUST）**適用於公共網際網路（例如**不得（MUST NOT）**僅適用於私有管理網路中的服務），除非：
   a. 金鑰使用方法之適用目的位於申請者能證明擁有其所有權之 OID arc 範圍內；或
   b. 申請者能以其他方式證明其有權於公共網際網路中聲明該金鑰使用方法之適用目的。
2. **不得（MUST NOT）**具有可能使信賴憑證者對 CA 所驗證之憑證資訊產生誤解的含義，例如宣稱私密金鑰儲存於智慧卡的金鑰使用方法之適用目的，而 CA 因採行遠端簽發，無法驗證對應之私密金鑰是否確實僅存在於該硬體內。
3. **應（MUST）**由簽發憑證機構（Issuing CA）驗證（即簽發憑證機構**應（MUST）**驗證交互認證之下屬憑證機構是否經授權得主張該金鑰使用方法之適用目的）。

CA **不得（MUST NOT）**包含額外的金鑰使用方法之適用目的，除非 CA 知悉有正當理由於憑證中包含該金鑰使用方法之適用目的。

### 7.1.2.2.6 交互認證之下屬憑證機構（Cross-Certified Subordinate CA）憑證之憑證原則

### （Certificate Policies）

憑證原則（Certificate Policies）擴充欄位**應（MUST）**包含至少一個 `PolicyInformation`。每個 `PolicyInformation` **應（MUST）**符合下列剖繪：

| 欄位 | 必要性 | 內容 |
|---|---|---|
| `policyIdentifier` | 應（MUST） | 當簽發憑證機構（Issuing CA）欲表示不存在何政策限制，且下屬憑證機構（Subordinate CA）為其關係企業時，簽發憑證機構**得（MAY）**使用 `anyPolicy` 政策識別碼；此時，憑證原則擴充欄位中**應（MUST）**僅包含此一 `PolicyInformation` 值。 |
| `anyPolicy` | 應（MUST） | |
| `policyQualifiers` | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**僅包含下表所列之允許 `policyQualifiers`。 |

無政策限制（適用於關係企業 CA）

| 欄位 | 必要性 | 內容 |
|---|---|---|
| `policyIdentifier` | 應（MUST） | 下列政策識別碼之一： |
| 保留憑證政策識別碼 | 應（MUST） | CA **應（MUST）**至少包含一個保留憑證政策識別碼（參見第 7.1.6.1 節），以對應由本憑證所代表之 CA 透過下屬 CA 間接簽發之指定用戶憑證類型（參見第 7.1.2.7.1 節）。 |
| `anyPolicy` | 不得（MUST NOT） | `anyPolicy` 政策識別碼**不得（MUST NOT）**存在。 |
| 任何其他識別碼 | 得（MAY） | 若存在，**應（MUST）**由 CA 定義，並載明於其憑證政策（CP）及／或憑證實務作業基準（CPS）中。 |
| `policyQualifiers` | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**僅包含下表所列之允許 `policyQualifiers`。 |

受政策限制

本剖繪**建議（RECOMMENDED）**憑證原則擴充欄位中之第一個 `PolicyInformation` 值包含保留憑證政策識別碼（參見第 7.1.6.1 節）[3]。無論 `PolicyInformation` 值之順序為何，憑證原則擴充欄位**應（MUST）**至少包含一個保留憑證政策識別碼。若有任何用戶憑證直接串鏈至依本憑證剖繪所簽發之憑證，則本交互認證之下屬憑證機構憑證**應（MUST）**包含僅有一個保留憑證政策識別碼。

**注意**：本憑證剖繪所簽發之任何憑證均**不建議（NOT RECOMMENDED）**包含 `policyQualifiers`，因為此資訊會增加憑證大小，但對一般信賴憑證者並無實質價值，且於必要時可透過其他方式取得。

若允許使用 `policyQualifiers`，且其存在於 `PolicyInformation` 欄位中，**應（MUST）**依下列格式編排：

| Qualifier ID | 必要性 | 欄位型別 | 內容 |
| --- | --- | --- | --- |
| `id-qt-cps`（OID：1.3.6.1.5.5.7.2.1） | 得（MAY） | `IA5String` | 簽發憑證機構（Issuing CA）之憑證政策（CP）、憑證實務作業基準（CPS）、信賴憑證者協議（Relying Party Agreement），或其他由簽發憑證機構提供的線上政策資訊之 HTTP 或 HTTPS URL。 |
| 任何其他 qualifier | 不得（MUST NOT） | - | - |

允許之 `policyQualifiers`

### 7.1.2.3 受技術約束之非 TLS 下屬憑證機構（Technically Constrained Non-TLS Subordinate CA）憑證剖繪

當簽發之 CA 憑證將被認定為受技術約束（Technically Constrained），且不會直接或間接用於簽發 TLS 憑證時，**得（MAY）**使用本憑證剖繪。

| 欄位 | 說明 |
| --- | --- |
| `tbsCertificate` | |
| `version` | **應（MUST）**為 v3(2) |
| `serialNumber` | **應（MUST）**為一個非連續之數值，其值大於 0 且小於 $2^{159}$，且其中至少 64 個位元應來自 CSPRNG 之輸出。 |
| `signature` | 參見第 7.1.3.2 節 |
| `issuer` | **應（MUST）**與簽發憑證機構（Issuing CA）之 `subject` 欄位逐位元組完全相同。參見第 7.1.4.1 節 |
| `validity` | 參見第 7.1.2.10.1 節 |
| `subject` | 參見第 7.1.2.10.2 節 |
| `subjectPublicKeyInfo` | 參見第 7.1.3.1 節 |
| `issuerUniqueID` | **不得（MUST NOT）**存在 |
| `subjectUniqueID` | **不得（MUST NOT）**存在 |
| `extensions` | 參見第 7.1.2.3.1 節 |
| `signatureAlgorithm` | 編碼後之值**應（MUST）**與 `tbsCertificate.signature` 逐位元組完全相同 |
| `signature` | |

#### 7.1.2.3.1 受技術約束之非 TLS 下屬憑證機構（Technically Constrained Non-TLS

### Subordinate CA）之擴充欄位

| 擴充欄位 | 必要性 | 關鍵性 | 說明 |
|---|---|---|---|
| `authorityKeyIdentifier` | 應（MUST） | N | 參見第 7.1.2.11.1 節 |
| `basicConstraints` | 應（MUST） | Y | 參見第 7.1.2.10.4 節 |
| `crlDistributionPoints` | 應（MUST） | N | 參見第 7.1.2.11.2 節 |
| `keyUsage` | 應（MUST） | Y | 參見第 7.1.2.10.7 節 |
| `subjectKeyIdentifier` | 應（MUST） | N | 參見第 7.1.2.11.4 節 |
| `extKeyUsage` | 應（MUST）[2] | N | 參見第 7.1.2.3.3 節 |
| `authorityInformationAccess` | 宜（SHOULD） | N | 參見第 7.1.2.10.3 節 |
| `certificatePolicies` | 得（MAY） | N | 參見第 7.1.2.3.2 節 |
| `nameConstraints` | 得（MAY） | *[1] | 參見第 7.1.2.10.8 節 |
| Signed Certificate Timestamp（SCT）清單 | 得（MAY） | N | 參見第 7.1.2.11.3 節 |
| 任何其他擴充欄位 | 不建議（NOT RECOMMENDED） | - | 參見第 7.1.2.11.5 節 |

### 7.1.2.3.2 受技術約束之非 TLS 下屬憑證機構（Technically Constrained Non-TLS Subordinate CA）之憑證原則（Certificate Policies）

若存在，憑證原則（Certificate Policies）擴充欄位**應（MUST）**依下列兩個表格其中之一的格式編排：

| 欄位 | 必要性 | 內容 |
|---|---|---|
| `policyIdentifier` | 應（MUST） | 當簽發憑證機構（Issuing CA）欲表示不存在何政策限制時，下屬憑證機構（Subordinate CA）**應（MUST）**為簽發憑證機構的關係企業。憑證原則擴充欄位**應（MUST）**僅包含一個 `PolicyInformation` 值，且該值**應（MUST）**包含 `anyPolicy` 政策識別碼。 |
| `anyPolicy` | 應（MUST） | |
| `policyQualifiers` | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**僅包含下表所列之允許 `policyQualifiers`。 |

無政策限制（適用於關係企業 CA）

| 欄位 | 必要性 | 內容 |
| --- | --- | --- |
| `policyIdentifier` | 應（MUST） | 下列政策識別碼之一： |
| 保留憑證政策識別碼 | 不得（MUST NOT） | |
| `anyPolicy` | 不得（MUST NOT） | `anyPolicy` 政策識別碼**不得（MUST NOT）**存在。 |
| 任何其他識別碼 | 得（MAY） | 若存在，**應（MUST）**由 CA 載明於其憑證政策（CP）及／或憑證實務作業基準（CPS）中。 |
| `policyQualifiers` | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**僅包含下表所列之允許 `policyQualifiers`。 |

受政策限制

| Qualifier ID | 必要性 | 欄位型別 | 內容 |
| --- | --- | --- | --- |
| `id-qt-cps`（OID：1.3.6.1.5.5.7.2.1） | 得（MAY） | `IA5String` | 簽發憑證機構（Issuing CA）之憑證政策（CP）、憑證實務作業基準（CPS）、信賴憑證者協議（Relying Party Agreement），或其他由簽發憑證機構提供的線上政策資訊之 HTTP 或 HTTPS URL。 |
| 任何其他 qualifier | 不得（MUST NOT） | - | - |

允許之 `policyQualifiers`

#### 7.1.2.3.3 受技術約束之非 TLS 下屬憑證機構（Technically Constrained Non-TLS Subordinate CA）之擴充金鑰使用方法（Extended Key Usage）

簽發憑證機構（Issuing CA）**應（MUST）**驗證下屬憑證機構憑證（Subordinate CA Certificate）是否經授權得針對該憑證所含之每項擴充金鑰使用方法之適用目的簽發憑證。**不建議（NOT RECOMMENDED）**包含多個彼此獨立的金鑰使用方法之適用目的（例如同時包含 `id-kp-timeStamping` 與 `id-kp-codeSigning`）。

| 金鑰適用目的（Key Purpose） | OID | 必要性 |
| --- | --- | --- |
| `id-kp-serverAuth` | 1.3.6.1.5.5.7.3.1 | 不得（MUST NOT） |
| `id-kp-OCSPSigning` | 1.3.6.1.5.5.7.3.9 | 不得（MUST NOT） |
| `anyExtendedKeyUsage` | 2.5.29.37.0 | 不得（MUST NOT） |
| 預簽憑證簽章憑證 | 1.3.6.1.4.1.11129.2.4.4 | 不得（MUST NOT） |
| 任何其他值 | - | 得（MAY） |

### 7.1.2.4 受技術約束之預簽憑證簽章憑證機構（Technically Constrained Precertificate

### Signing CA）憑證剖繪

當簽發一張將用作 RFC 6962 第 3.1 節 所述之預簽憑證簽章憑證機構（Precertificate Signing CA）之 CA 憑證時，**應（MUST）**使用本憑證剖繪。若該 CA 憑證符合本剖繪，則視為受技術約束（Technically Constrained）。

預簽憑證簽章憑證機構（Precertificate Signing CA）**應（MUST）**僅用於簽章第 7.1.2.9 節所定義之預簽憑證。當預簽憑證簽章憑證機構簽發預簽憑證時，應將其解釋為：在規範上視同該預簽憑證簽章憑證機構（Precertificate Signing CA）的簽發憑證機構（Issuing CA），已簽發一張有效憑證；該有效憑證之 `tbsCertificate` 與依照 RFC 6962 第 3.2 節 規定之修改套用後的相對應預簽憑證之 `tbsCertificate` 相符。

如 RFC 6962 第 3.2 節 所述，預簽憑證的 `signature` 欄位不會因上述修改而改變。因此，預簽憑證簽章憑證機構（Precertificate Signing CA）在簽發預簽憑證時，**應（MUST）**使用與簽發憑證機構（Issuing CA）相同之簽章演算法；同樣地，其公開金鑰**應（MUST）**使用與簽發憑證機構（Issuing CA）相同之公開金鑰演算法，但**得（MAY）**使用不同之 CA 金鑰對。

| 欄位 | 說明 |
|---|---|
| `tbsCertificate` | |
| `version` | **應（MUST）**為 v3(2) |
| `serialNumber` | **應（MUST）**為一個非連續之數值，其值大於 0 且小於 $2^{159}$，且其中至少 64 個位元應來自 CSPRNG 之輸出。 |
| `signature` | 參見第 7.1.3.2 節 |
| `issuer` | **應（MUST）**與簽發憑證機構（Issuing CA）之 `subject` 欄位逐位元組完全相同。參見第 7.1.4.1 節 |
| `validity` | 參見第 7.1.2.10.1 節 |
| `subject` | 參見第 7.1.2.10.2 節 |
| `subjectPublicKeyInfo` | 演算法識別碼（algorithm identifier）**應（MUST）**與簽發憑證機構（Issuing CA）的 `subjectPublicKeyInfo` 欄位中之演算法識別碼逐位元組完全相同。參見第 7.1.3.1 節 |
| `issuerUniqueID` | **不得（MUST NOT）**存在 |
| `subjectUniqueID` | **不得（MUST NOT）**存在 |
| `extensions` | 參見第 7.1.2.4.1 節 |
| `signatureAlgorithm` | 編碼後之值**應（MUST）**與 `tbsCertificate.signature` 逐位元組完全相同 |
| `signature` | |

自 2026-03-15 起：

- 本憑證剖繪**不得（MUST NOT）**使用。
- 預簽憑證簽章憑證機構（Precertificate Signing CA）**不得（MUST NOT）**用於簽發預簽憑證。

#### 7.1.2.4.1 受技術約束之預簽憑證簽章憑證機構（Technically Constrained Precertificate Signing CA）之擴充欄位

| 擴充欄位 | 必要性 | 關鍵性 | 說明 |
|---|---|---|---|
| `authorityKeyIdentifier` | 應（MUST） | N | 參見第 7.1.2.11.1 節 |
| `basicConstraints` | 應（MUST） | Y | 參見第 7.1.2.10.4 節 |
| `certificatePolicies` | 應（MUST） | N | 參見第 7.1.2.10.5 節 |
| `crlDistributionPoints` | 應（MUST） | N | 參見第 7.1.2.11.2 節 |
| `keyUsage` | 應（MUST） | Y | 參見第 7.1.2.10.7 節 |
| `subjectKeyIdentifier` | 應（MUST） | N | 參見第 7.1.2.11.4 節 |
| `extKeyUsage` | 應（MUST）[2] | N | 參見第 7.1.2.4.2 節 |
| `authorityInformationAccess` | 宜（SHOULD） | N | 參見第 7.1.2.10.3 節 |
| `nameConstraints` | 得（MAY） | *[1] | 參見第 7.1.2.10.8 節 |
| Signed Certificate Timestamp（SCT）清單 | 得（MAY） | N | 參見第 7.1.2.11.3 節 |
| 任何其他擴充欄位 | 不建議（NOT RECOMMENDED） | - | 參見第 7.1.2.11.5 節 |

#### 7.1.2.4.2 受技術約束之預簽憑證簽章憑證機構（Technically Constrained Precertificate Signing CA）之擴充金鑰使用方法（Extended Key Usage）

| 金鑰適用目的（Key Purpose） | OID | 必要性 |
|---|---|---|
| 預簽憑證簽章憑證 | 1.3.6.1.4.1.11129.2.4.4 | 應（MUST） |
| 任何其他值 | - | 不得（MUST NOT） |

### 7.1.2.5 受技術約束之 TLS 下屬憑證機構（Technically Constrained TLS Subordinate CA）憑證剖繪

當簽發之 CA 憑證將被認定為受技術約束（Technically Constrained），且將直接或間接用於簽發 TLS 憑證時，**得（MAY）**使用本憑證剖繪。

| 欄位 | 說明 |
| --- | --- |
| `tbsCertificate` | |
| `version` | **應（MUST）**為 v3(2) |
| `serialNumber` | **應（MUST）**為一個非連續之數值，其值大於 0 且小於 $2^{159}$，且其中至少 64 個位元應來自 CSPRNG 之輸出。 |
| `signature` | 參見第 7.1.3.2 節 |
| `issuer` | **應（MUST）**與簽發憑證機構（Issuing CA）之 `subject` 欄位逐位元組完全相同。參見第 7.1.4.1 節 |
| `validity` | 參見第 7.1.2.10.1 節 |
| `subject` | 參見第 7.1.2.10.2 節 |
| `subjectPublicKeyInfo` | 參見第 7.1.3.1 節 |
| `issuerUniqueID` | **不得（MUST NOT）**存在 |
| `subjectUniqueID` | **不得（MUST NOT）**存在 |
| `extensions` | 參見第 7.1.2.5.1 節 |
| `signatureAlgorithm` | 編碼後之值**應（MUST）**與 `tbsCertificate.signature` 逐位元組完全相同 |
| `signature` | |

#### 7.1.2.5.1 受技術約束之 TLS 下屬憑證機構（Technically Constrained TLS Subordinate CA）

之擴充欄位

| 擴充欄位 | 必要性 | 關鍵性 | 說明 |
| --- | --- | --- | --- |
| `authorityKeyIdentifier` | 應（MUST） | N | 參見第 7.1.2.11.1 節 |
| `basicConstraints` | 應（MUST） | Y | 參見第 7.1.2.10.4 節 |
| `certificatePolicies` | 應（MUST） | N | 參見第 7.1.2.10.5 節 |
| `crlDistributionPoints` | 應（MUST） | N | 參見第 7.1.2.11.2 節 |
| `keyUsage` | 應（MUST） | Y | 參見第 7.1.2.10.7 節 |
| `subjectKeyIdentifier` | 應（MUST） | N | 參見第 7.1.2.11.4 節 |
| `extKeyUsage` | 應（MUST）[2] | N | 參見第 7.1.2.10.6 節 |
| `nameConstraints` | 應（MUST） | *[1] | 參見第 7.1.2.5.2 節 |
| `authorityInformationAccess` | 宜（SHOULD） | N | 參見第 7.1.2.10.3 節 |
| Signed Certificate Timestamp（SCT）清單 | 得（MAY） | N | 參見第 7.1.2.11.3 節 |
| 任何其他擴充欄位 | 不建議（NOT RECOMMENDED） | - | 參見第 7.1.2.11.5 節 |

#### 7.1.2.5.2 受技術約束之 TLS 下屬憑證機構（Technically Constrained Non-TLS Subordinate CA）之名稱限制（Name Constraints）

TLS 下屬憑證機構（Subordinate CA）若欲成為受技術約束（Technically Constrained），名稱限制（Name Constraints）擴充欄位**應（MUST）**依以下方式編碼。作為 RFC 5280 之明確例外，本擴充欄位**宜（SHOULD）**標記為關鍵（critical），但若需與某些不支援名稱限制之舊版應用程式相容，**得（MAY）**標記為非關鍵（non-critical）。

| 欄位 | 說明 |
| --- | --- |
| permittedSubtrees | permittedSubtrees **應（MUST）**對每一種 dNSName 與 iPAddress GeneralName 名稱類型，各包含至少一個 GeneralSubtree，除非該 GeneralName 名稱類型已出現於 excludedSubtrees 中，用以排除該名稱類型之所有值。此外，permittedSubtrees **應（MUST）**包含至少一個 directoryName GeneralName 名稱類型的 GeneralSubtree。 |
| GeneralSubtree | 符合 permittedSubtrees 中各 GeneralSubtree 之要求規定。 |
| base | 參見下表 |
| minimum | **不得（MUST NOT）**存在 |
| maximum | **不得（MUST NOT）**存在 |
| excludedSubtrees | excludedSubtrees **應（MUST）**對每一種 dNSName 與 iPAddress GeneralName 名稱類型，各包含至少一個 GeneralSubtree，除非 permittedSubtrees 中已包含該名稱類型的 GeneralSubtree。不建議（NOT RECOMMENDED）使用 directoryName 名稱類型。 |
| GeneralSubtree | 符合 permittedSubtrees 中各 GeneralSubtree 之要求規定。 |
| base | 參見下表 |
| minimum | **不得（MUST NOT）**存在 |
| maximum | **不得（MUST NOT）**存在 |

nameConstraints 要求規定

下表列出 permittedSubtrees 或 excludedSubtrees 中各 GeneralSubtree 之 base 所包含的 GeneralName 要求規定。

| GeneralName 名稱類型 | 必要性 | permittedSubtrees | excludedSubtrees | 排除該類型整個 Namespace |
|---|---|---|---|---|
| dNSName | 應（MUST） | CA **應（MUST）**確認申請者已註冊該 dNSName，或已獲網域名稱註冊人授權代表該註冊人行事。參見第 3.2.2.4 節。 | 若 permittedSubtrees 中至少存在一個 dNSName，CA **得（MAY）**於 excludedSubtrees 指定 dNSName 網域之一個或多個子網域名稱作為欲排除項目。 | 若 permittedSubtrees 中不存在任何 dNSName，CA **應（MUST）**於 permittedSubtrees 包含一個零長度（空字串）的 dNSName，以表示不允許任何網域名稱。 |
| iPAddress | 應（MUST） | CA **應（MUST）**確認申請者已被指配該 iPAddress 範圍，或已獲 IP 位址分配者（assigner）授權代表被指配者（assignee）行事。參見第 3.2.2.5 節。 | 若 permittedSubtrees 中至少存在一個 iPAddress，CA **得（MAY）**於 excludedSubtrees 指定該等 iPAddress 範圍內之一個或多個子網段作為欲排除項目。 | 若 permittedSubtrees 中未包含任何 IPv4 iPAddress，CA **應（MUST）**於 permittedSubtrees 包含一個由 8 個零位元組組成的 iPAddress，表示排除整個 IPv4 位址範圍（0.0.0.0/0）。若 permittedSubtrees 中未包含任何 IPv6 iPAddress，CA **應（MUST）**於 permittedSubtrees 包含一個由 32 個零位元組組成的 iPAddress，表示排除整個 IPv6 位址範圍（::0/0）。 |
| directoryName | 應（MUST） | CA **應（MUST）**確認申請者及／或其子公司之名稱屬性，以確保所有簽發之憑證均遵循相關憑證剖繪（參見第 7.1.2 節），包含名稱形式（參見第 7.1.4 節）。 | 不建議（NOT RECOMMENDED）於 excludedSubtrees 中包含任何值。 | CA **應（MUST）**於 permittedSubtrees 中包含一個值，因此本欄位不適用。詳見 excludedSubtrees 之相關規定。 |
| otherName | 不建議（NOT RECOMMENDED） | 參見下文 | 參見下文 | 參見下文 |
| 任何其他值 | 不得（MUST NOT） | - | - | - |

base 欄位所包含之 GeneralName 要求規定

任何 otherName，若存在：

1. **應（MUST）**適用於公共網際網路，除非：
   a. type-id 位於申請者能證明擁有其所有權之 OID arc 範圍內，或
   b. 申請者能以其他方式證明其有權於公共網際網路中聲明該資料。
2. **不得（MUST NOT）**具有可能使信賴憑證者對 CA 所驗證之憑證資訊產生誤解的含義。
3. **應（MUST）**依相關 ASN.1 模組中對該 otherName 的 type-id 與 value 之定義，以 DER 進行編碼。

CA **不得（SHALL NOT）**包含額外名稱（例如額外的 GeneralName），除非 CA 知悉有正當理由於憑證中包含該資料。

### 7.1.2.6 TLS 下屬憑證機構（TLS Subordinate CA）憑證剖繪

| 欄位 | 說明 |
|---|---|
| tbsCertificate | |
| version | **應（MUST）**為 v3(2) |
| serialNumber | **應（MUST）**為一個非連續之數值，其值大於 0 且小於 $2^{159}$，且其中至少 64 個位元應來自 CSPRNG 之輸出。 |
| signature | 參見第 7.1.3.2 節 |
| issuer | **應（MUST）**與簽發憑證機構（Issuing CA）之 subject 欄位逐位元組完全相同。參見第 7.1.4.1 節 |
| validity | 參見第 7.1.2.10.1 節 |
| subject | 參見第 7.1.2.10.2 節 |
| subjectPublicKeyInfo | 參見第 7.1.3.1 節 |
| issuerUniqueID | **不得（MUST NOT）**存在 |
| subjectUniqueID | **不得（MUST NOT）**存在 |
| extensions | 參見第 7.1.2.6.1 節 |
| signatureAlgorithm | 編碼後之值**應（MUST）**與 tbsCertificate.signature 逐位元組完全相同 |
| signature | |

#### 7.1.2.6.1 TLS 下屬憑證機構（TLS Subordinate CA Extensions）之擴充欄位

| 擴充欄位 | 必要性 | 關鍵性 | 說明 |
|---|---|---|---|
| `authorityKeyIdentifier` | 應（MUST） | N | 參見第 7.1.2.11.1 節 |
| `basicConstraints` | 應（MUST） | Y | 參見第 7.1.2.10.4 節 |
| `certificatePolicies` | 應（MUST） | N | 參見第 7.1.2.10.5 節 |
| `crlDistributionPoints` | 應（MUST） | N | 參見第 7.1.2.11.2 節 |
| `keyUsage` | 應（MUST） | Y | 參見第 7.1.2.10.7 節 |
| `subjectKeyIdentifier` | 應（MUST） | N | 參見第 7.1.2.11.4 節 |
| `extKeyUsage` | 應（MUST）[2] | N | 參見第 7.1.2.10.6 節 |
| `authorityInformationAccess` | 宜（SHOULD） | N | 參見第 7.1.2.10.3 節 |
| `nameConstraints` | 得（MAY） | *[1] | 參見第 7.1.2.10.8 節 |
| Signed Certificate Timestamp（SCT）清單 | 得（MAY） | N | 參見第 7.1.2.11.3 節 |
| 任何其他擴充欄位 | 不建議（NOT RECOMMENDED） | - | 參見第 7.1.2.11.5 節 |

### 7.1.2.7 用戶（伺服器）（Subscriber (Server)）憑證剖繪

| 欄位 | 說明 |
|---|---|
| tbsCertificate | |
| version | **應（MUST）**為 v3(2) |
| serialNumber | **應（MUST）**為一個非連續之數值，其值大於 0 且小於 $2^{159}$，且其中至少 64 個位元應來自 CSPRNG 之輸出。 |
| signature | 參見第 7.1.3.2 節 |
| issuer | **應（MUST）**與簽發憑證機構（Issuing CA）之 subject 欄位逐位元組完全相同。參見第 7.1.4.1 節 |
| validity | |
| notBefore | 與憑證簽章作業時間點相差不超過 48 小時之值。 |
| notAfter | 參見第 6.3.2 節 |
| subject | 參見第 7.1.2.7.1 節 |
| subjectPublicKeyInfo | 參見第 7.1.3.1 節 |
| issuerUniqueID | **不得（MUST NOT）**存在 |
| subjectUniqueID | **不得（MUST NOT）**存在 |
| extensions | 參見第 7.1.2.7.6 節 |
| signatureAlgorithm | 編碼後之值**應（MUST）**與 tbsCertificate.signature 逐位元組完全相同 |
| signature | |

#### 7.1.2.7.1 用戶憑證（Subscriber Certificate）類型

可簽發四種類型之用戶憑證，其類型依所包含之主體資訊（Subject Information）多寡而有所不同。各類型憑證均採用相同剖繪，但有三項例外：可出現之 subject 名稱欄位、這些欄位的驗證方法，以及 certificatePolicies 擴充欄位之內容。

| 類型 | 說明 |
|---|---|
| 網域驗證型（Domain Validated，DV） | 參見第 7.1.2.7.2 節 |
| 個人驗證型（Individual Validated，IV） | 參見第 7.1.2.7.3 節 |
| 組織驗證型（Organization Validated，OV） | 參見第 7.1.2.7.4 節 |
| 延伸驗證型（Extended Validation，EV） | 參見第 7.1.2.7.5 節 |

**注意**：雖然各類型用戶憑證所包含之主體資訊有所不同，但所有憑證對裝置身分（網域名稱及／或 IP 位址）均提供相同保證等級。

#### 7.1.2.7.2 網域驗證型（DV）用戶憑證剖繪

若用戶憑證屬於網域驗證型（Domain Validated）憑證，**應（MUST）**符合下列剖繪：

| 欄位 | 要求 |
| --- | --- |
| `subject` | 參見下表 |
| `certificatePolicies` | **應（MUST）**存在。**應（MUST）**使用 `policyIdentifier` 宣告保留憑證政策識別碼 `2.23.140.1.2.1`。參見第 7.1.2.7.9 節。 |
| 所有其他擴充欄位 | 參見第 7.1.2.7.6 節 |

所有 `subject` 名稱**應（MUST）**依第 7.1.4 節規定之方式編碼。

下表列出 `AttributeTypeAndValue` 之 `type` 欄位允許使用的 `AttributeType`，以及對應之 `value` 欄位允許填列的內容。

| `AttributeType` 屬性名稱 | 必要性 | `value` | 驗證方法 |
| --- | --- | --- | --- |
| `countryName` | 得（MAY） | 與主體關聯之國家的兩字母 ISO 3166-1 國家代碼。 | 第 3.2.2.3 節 |
| `commonName` | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**包含依第 7.1.4.3 節規定，取自 `subjectAltName` 擴充欄位之值。 | |
| 任何其他屬性 | 不得（MUST NOT） | - | - |

網域驗證型憑證之 `subject` 屬性

#### 7.1.2.7.3 個人驗證型（IV）用戶憑證剖繪

若用戶憑證屬於個人驗證型（Individual Validated）憑證，**應（MUST）**符合下列剖繪：

| 欄位 | 要求 |
| --- | --- |
| `subject` | 參見下表 |
| `certificatePolicies` | **應（MUST）**存在。**應（MUST）**使用 `policyIdentifier` 宣告保留憑證政策識別碼 `2.23.140.1.2.3`。參見第 7.1.2.7.9 節。 |
| 所有其他擴充欄位 | 參見第 7.1.2.7.6 節 |

所有 `subject` 名稱**應（MUST）**依第 7.1.4 節規定之方式編碼。

下表列出 `AttributeTypeAndValue` 之 `type` 欄位允許使用的 `AttributeType`，以及對應之 `value` 欄位允許填列的內容。

| AttributeType 屬性名稱 | 必要性 | value | 驗證方法 |
| --- | --- | --- | --- |
| countryName | 應（MUST） | 與主體關聯之國家的兩字母 ISO 3166-1 國家代碼。若該國家未獲正式 ISO 3166-1 國家代碼，CA **應（MUST）**指定 ISO 3166-1 使用者保留代碼 xx，以表示尚未被分配正式 ISO 3166-1 雙字母代碼。 | 第 3.2.3 節 |
| stateOrProvinceName | 應（MUST）／得（MAY） | 若 localityName 不存在，此欄位**應（MUST）**存在；否則，此欄位**得（MAY）**存在。若存在，**應（MUST）**包含主體之州或省資訊。 | 第 3.2.3 節 |
| localityName | 應（MUST）／得（MAY） | 若 stateOrProvinceName 不存在，此欄位**應（MUST）**存在；否則，此欄位**得（MAY）**存在。若存在，**應（MUST）**包含主體之縣市地區資訊。 | 第 3.2.3 節 |
| postalCode | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**包含主體之郵遞區號資訊。 | 第 3.2.3 節 |
| streetAddress | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**包含主體之街道地址資訊。**得（MAY）**包含多個實體地址。 | 第 3.2.3 節 |
| organizationName | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**包含主體之名稱及／或商業名稱／商標名稱（DBA/tradename）。CA **得（MAY）**在此欄位包含與已驗證名稱略有出入之資訊，例如常見之變體或縮寫，前提是 CA 須以書面文件記錄其差異及所使用之縮寫為當地公認之縮寫。若主體之名稱與商業名稱兩者均包含，商業名稱／商標名稱**應（SHALL）**排列在前，其後以括號附上主體名稱。 | 第 3.2.3 節 |
| surname | 應（MUST） | 主體之姓氏 | 第 3.2.3 節 |
| givenName | 應（MUST） | 主體之名字 | 第 3.2.3 節 |
| organizationalUnitName | 不得（MUST NOT） | - | - |
| commonName | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**包含依第 7.1.4.3 節規定，取自 subjectAltName 擴充欄位之值。 | |

| AttributeType 屬性名稱 | 必要性 | value | 驗證方法 |
| --- | --- | --- | --- |
| 任何其他屬性 | 不建議（NOT RECOMMENDED） | - | 參見第 7.1.4.4 節 |

個人驗證型憑證之 subject 屬性

此外，subject 屬性**不得（MUST NOT）**僅包含「.」、「-」及空格（space）等占位符號，及／或任何其他表示該屬性值不存在、不完整或不適用之內容。

### 7.1.2.7.4 組織驗證型（OV）用戶憑證剖繪

若用戶憑證屬於組織驗證型（Organization Validated）憑證，**應（MUST）**符合下列剖繪：

| 欄位 | 要求 |
| --- | --- |
| subject | 參見下表 |
| certificatePolicies | **應（MUST）**存在。**應（MUST）**使用 policyIdentifier 宣告保留憑證政策識別碼 2.23.140.1.2.2。參見第 7.1.2.7.9 節。 |
| 所有其他擴充欄位 | 參見第 7.1.2.7.6 節 |

所有 subject 名稱**應（MUST）**依第 7.1.4 節規定之方式編碼。

下表列出 AttributeTypeAndValue 之 type 欄位允許使用的 AttributeType，以及對應之 value 欄位允許填列的內容。

| AttributeType 屬性名稱 | 必要性 | value | 驗證方法 |
| --- | --- | --- | --- |
| domainComponent | 得（MAY） | 若存在，此欄位**應（MUST）**包含網域名稱中之一個網域標籤（Domain Label）。該網域名稱的所有網域標籤**應（MUST）**以單一有序之序列表示於 domainComponent 欄位中。網域標籤**應（MUST）**按照與 DNS 協定之網域名稱線路傳輸（on-wire）表示相反之順序編碼，使最接近根（root）節點之網域標籤最先編碼。**得（MAY）**包含多個 domainComponent 實例。 | 第 3.2 節 |
| countryName | 應（MUST） | 與主體關聯之國家的兩字母 ISO 3166-1 國家代碼。若該國家未獲正式 ISO 3166-1 國家代碼，CA **應（MUST）**指定 ISO 3166-1 使用者保留代碼 xx，以表示尚未被分配正式 ISO 3166-1 雙字母代碼。 | 第 3.2.2.1 節 |
| stateOrProvinceName | 應（MUST）／得（MAY） | 若 localityName 不存在，此欄位**應（MUST）**存在；否則，此欄位**得（MAY）**存在。若存在，**應（MUST）**包含主體之州或省資訊。 | 第 3.2.2.1 節 |
| localityName | 應（MUST）／得（MAY） | 若 stateOrProvinceName 不存在，此欄位**應（MUST）**存在；否則，此欄位**得（MAY）**存在。若存在，**應（MUST）**包含主體之縣市地區資訊。 | 第 3.2.2.1 節 |
| postalCode | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**包含主體之郵遞區號資訊。 | 第 3.2.2.1 節 |
| streetAddress | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**包含主體之街道地址資訊。**得（MAY）**包含多個實體地址。 | 第 3.2.2.1 節 |

| AttributeType 屬性名稱 | 必要性 | value | 驗證方法 |
| --- | --- | --- | --- |
| organizationName | 應（MUST） | 主體之名稱及／或商業名稱／商標名稱（DBA/tradename）。CA **得（MAY）**在此欄位包含與已驗證名稱略有出入之資訊，例如常見之變體或縮寫，前提是 CA 須以書面文件記錄其差異及所使用之縮寫為當地公認之縮寫；例如：若官方記錄顯示為「Company Name Incorporated」，CA **得（MAY）**使用「Company Name Inc.」或「Company Name」。若主體之名稱與商業名稱兩者均包含，商業名稱／商標名稱**應（SHALL）**排列在前，其後以括號附上主體名稱。 | 第 3.2.2.2 節 |
| surname | 不得（MUST NOT） | - | - |
| givenName | 不得（MUST NOT） | - | - |
| organizationalUnitName | 不得（MUST NOT） | - | - |
| commonName | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**包含依第 7.1.4.3 節規定，取自 subjectAltName 擴充欄位之值。 | |
| 任何其他屬性 | 不建議（NOT RECOMMENDED） | - | 參見第 7.1.4.4 節 |

組織驗證型憑證之 subject 屬性

此外，subject 屬性**不得（MUST NOT）**僅包含「.」、「-」及空格（space）等占位符號，及／或任何其他表示該屬性值不存在、不完整或不適用之內容。

### 7.1.2.7.5 延伸驗證型（EV）用戶憑證剖繪

若用戶憑證屬於延伸驗證型（Extended Validation）憑證，**應（MUST）**遵循當時有效版本之《延伸驗證型憑證之簽發與管理指引》（the Guidelines for the Issuance and Management of Extended Validation Certificates）所規定的憑證剖繪。

此外，**應（MUST）**符合下列剖繪：

| 欄位 | 要求 |
| --- | --- |
| `subject` | 參見《延伸驗證型憑證之簽發與管理指引》第 7.1.4.2 節 |
| `certificatePolicies` | **應（MUST）**存在。**應（MUST）**使用 `policyIdentifier` 宣告保留憑證政策識別碼 `2.23.140.1.1`。參見第 7.1.2.7.9 節 |
| 所有其他擴充欄位 | 參見第 7.1.2.7.6 節及《延伸驗證型憑證之簽發與管理指引》 |

此外，`subject` 屬性**不得（MUST NOT）**僅包含「.」、「-」及空格（space）等占位符號，及／或任何其他表示該屬性值不存在、不完整或不適用之內容。

### 7.1.2.7.6 用戶憑證（Subscriber Certificate）之擴充欄位

| 擴充欄位 | 必要性 | 關鍵性 | 說明 |
| --- | --- | --- | --- |
| `authorityInformationAccess` | 應（MUST） | N | 參見第 7.1.2.7.7 節 |
| `authorityKeyIdentifier` | 應（MUST） | N | 參見第 7.1.2.11.1 節 |
| `certificatePolicies` | 應（MUST） | N | 參見第 7.1.2.7.9 節 |
| `extKeyUsage` | 應（MUST） | N | 參見第 7.1.2.7.10 節 |
| `subjectAltName` | 應（MUST） | * | 參見第 7.1.2.7.12 節 |
| `nameConstraints` | 不得（MUST NOT） | - | - |
| `keyUsage` | 宜（SHOULD） | Y | 參見第 7.1.2.7.11 節 |
| `basicConstraints` | 得（MAY） | Y | 參見第 7.1.2.7.8 節 |
| `crlDistributionPoints` | * | N | 參見第 7.1.2.11.2 節 |
| Signed Certificate Timestamp（SCT）清單 | 得（MAY） | N | 參見第 7.1.2.11.3 節 |
| `subjectKeyIdentifier` | 不建議（NOT RECOMMENDED） | N | 參見第 7.1.2.11.4 節 |
| 任何其他擴充欄位 | 不建議（NOT RECOMMENDED） | - | 參見第 7.1.2.11.5 節 |

**注意**：

- `subjectAltName` 擴充欄位是否應標記為關鍵（Critical），取決於憑證 `subject` 欄位之內容，詳見第 7.1.2.7.12 節。
- CRL Distribution Points（CRL 發布點）擴充欄位是否應存在，取決於：（1）憑證是否包含 accessMethod 為 `id-ad-ocsp` 之 Authority Information Access（AIA）擴充欄位，以及（2）憑證之有效期，詳見第 7.1.2.11.2 節。

#### 7.1.2.7.7 用戶憑證（Subscriber Certificate）之憑證機構資訊存取（Authority Information Access）

`AuthorityInfoAccessSyntax` **應（MUST）**包含一個或多個 `AccessDescription`。每個 `AccessDescription` **應（MUST）**僅包含下表所列之允許 `accessMethod`，且每個 `accessLocation` **應（MUST）**編碼為指定之 `GeneralName` 型別。

若該 `accessMethod` 允許指定多個 `AccessDescription`，`AuthorityInfoAccessSyntax` **得（MAY）**包含多個具有相同 `accessMethod` 的 `AccessDescription`。當存在多個具有相同 `accessMethod` 的 `AccessDescription` 時，各 `accessLocation` **應（MUST）**互不相同，且各 `AccessDescription` **應（MUST）**依該 `accessMethod` 之優先順位排列，其中具有最高優先順位 `accessLocation` 的 `AccessDescription` 應排列於首位。在符合前述要求之前提下，對於具有不同 `accessMethod` 的 `AccessDescription`，不另定其排序要求。

| accessMethod | accessLocation | 必要性 | 最大數量 | 說明 |
|---|---|---|---|---|
| `id-ad-ocsp`（OID：1.3.6.1.5.5.7.48.1） | `uniformResourceIdentifier` | 得（MAY） | *（任意數量） | 簽發憑證機構（Issuing CA）的 OCSP 回應伺服器 HTTP URL。 |
| `id-ad-caIssuers`（OID：1.3.6.1.5.5.7.48.2） | `uniformResourceIdentifier` | 宜（SHOULD） | *（任意數量） | 簽發憑證機構憑證的 HTTP URL。 |
| 任何其他值 | - | 不得（MUST NOT） | - | 不得使用其他 `accessMethod`。 |

#### 7.1.2.7.8 用戶憑證（Subscriber Certificate）之基本限制（Basic Constraints）

| 欄位 | 說明 |
|---|---|
| `cA` | **應（MUST）**為 FALSE |
| `pathLenConstraint` | **不得（MUST NOT）**存在 |

#### 7.1.2.7.9 用戶憑證（Subscriber Certificate）之憑證原則（Certificate Policies）

若存在，憑證原則（Certificate Policies）擴充欄位**應（MUST）**包含至少一個 `PolicyInformation`。每個 `PolicyInformation` **應（MUST）**符合下列剖繪：

| 欄位 | 必要性 | 內容 |
| --- | --- | --- |
| `policyIdentifier` | 應（MUST） | 下列政策識別碼之一： |
| 保留憑證政策識別碼 | 應（MUST） | 與指定用戶憑證類型（參見第 7.1.2.7.1 節）相對應之保留憑證政策識別碼（參見第 7.1.6.1 節）。 |
| `anyPolicy` | 不得（MUST NOT） | `anyPolicy` 政策識別碼**不得（MUST NOT）**存在。 |
| 任何其他識別碼 | 得（MAY） | 若存在，**應（MUST）**由 CA 定義，並載明於其憑證政策（CP）及／或憑證實務作業基準（CPS）中。 |
| `policyQualifiers` | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**僅包含下表所列之允許 `policyQualifiers`。 |

本剖繪**建議（RECOMMENDED）**憑證原則擴充欄位中之第一個 `PolicyInformation` 值包含保留憑證政策識別碼（參見第 7.1.6.1 節）[3]。無論 `PolicyInformation` 值之順序為何，憑證原則擴充欄位**應（MUST）**包含僅有一個保留憑證政策識別碼。

| Qualifier ID | 必要性 | 欄位型別 | 內容 |
| --- | --- | --- | --- |
| `id-qt-cps`（OID：1.3.6.1.5.5.7.2.1） | 得（MAY） | `IA5String` | 簽發憑證機構（Issuing CA）之憑證政策（CP）、憑證實務作業基準（CPS）、信賴憑證者協議（Relying Party Agreement），或其他由簽發憑證機構提供的線上政策資訊之 HTTP 或 HTTPS URL。 |
| 任何其他 qualifier | 不得（MUST NOT） | - | - |

允許之 `policyQualifiers`

### 7.1.2.7.10 用戶憑證（Subscriber Certificate）之擴充金鑰使用方法（Extended Key

### Usage）

| 金鑰適用目的（Key Purpose） | OID | 必要性 |
| --- | --- | --- |
| `id-kp-serverAuth` | 1.3.6.1.5.5.7.3.1 | 應（MUST） |
| `id-kp-clientAuth` | 1.3.6.1.5.5.7.3.2 | 得（MAY） |
| `id-kp-codeSigning` | 1.3.6.1.5.5.7.3.3 | 不得（MUST NOT） |
| `id-kp-emailProtection` | 1.3.6.1.5.5.7.3.4 | 不得（MUST NOT） |
| `id-kp-timeStamping` | 1.3.6.1.5.5.7.3.8 | 不得（MUST NOT） |
| `id-kp-OCSPSigning` | 1.3.6.1.5.5.7.3.9 | 不得（MUST NOT） |
| `anyExtendedKeyUsage` | 2.5.29.37.0 | 不得（MUST NOT） |
| 預簽憑證簽章憑證 | 1.3.6.1.4.1.11129.2.4.4 | 不得（MUST NOT） |
| 任何其他值 | - | 不建議（NOT RECOMMENDED） |

### 7.1.2.7.11 用戶憑證（Subscriber Certificate）之憑證金鑰用途（Key Usage）

可接受之憑證金鑰用途欄位值，視憑證之 `subjectPublicKeyInfo` 識別欄位為 RSA 公開金鑰或 ECC 公開金鑰而定。CA **應（MUST）**確保憑證金鑰用途之設定符合憑證公開金鑰之用途。

| 憑證金鑰用途（Key Usage） | 可否設定 | 設定必要性 |
| --- | --- | --- |
| `digitalSignature` | Y | 宜（SHOULD） |
| `nonRepudiation` | N | — |
| `keyEncipherment` | Y | 得（MAY） |
| `dataEncipherment` | Y | 不建議（NOT RECOMMENDED） |
| `keyAgreement` | N | — |
| `keyCertSign` | N | — |
| `cRLSign` | N | — |
| `encipherOnly` | N | — |
| `decipherOnly` | N | — |

RSA 公開金鑰之憑證金鑰用途

**注意**：RSA 公開金鑰**應（MUST）**設定至少一種憑證金鑰用途。使用現代通訊協定（如 TLS 1.3）及安全加密套件時，設定 `digitalSignature` 旗標位元為**必要（REQUIRED）**項目；使用不安全加密套件時，為了支援較舊通訊協定（如 TLS 1.2），**得（MAY）**設定 `keyEncipherment` 旗標位元。用戶**得（MAY）**考量採用金鑰隔離，以降低此類舊有協定所帶來的風險，因此 CA **得（MAY）**簽發僅設定 `keyEncipherment` 旗標位元之用戶憑證。對多數用戶而言，設定 `digitalSignature` 旗標位元已足夠；若用戶希望以相同演算法同時使用不安全與安全的加密套件，可選擇在同一憑證中同時設定 `digitalSignature` 與 `keyEncipherment` 旗標位元，但**不建議（NOT RECOMMENDED）**採用此方式。`dataEncipherment` 旗標位元目前仍允許設定，但**不建議（NOT RECOMMENDED）**設定該旗標位元，因其屬於預告禁用（Pending Prohibition）項目（https://github.com/cabforum/servercert/issues/384）。

| 憑證金鑰用途（Key Usage） | 可否設定 | 設定必要性 |
|---|---|---|
| `digitalSignature` | Y | 應（MUST） |
| `nonRepudiation` | N | — |
| `keyEncipherment` | N | — |
| `dataEncipherment` | N | — |
| `keyAgreement` | Y | 不建議（NOT RECOMMENDED） |
| `keyCertSign` | N | — |
| `cRLSign` | N | — |
| `encipherOnly` | N | — |
| `decipherOnly` | N | — |

ECC 公開金鑰之憑證金鑰用途

**注意**：`keyAgreement` 旗標位元目前仍允許設定，但**不建議（NOT RECOMMENDED）**設定該旗標位元，因其屬於預告禁用（Pending Prohibition）項目（https://github.com/cabforum/servercert/issues/384）。

### 7.1.2.7.12 用戶憑證（Subscriber Certificate）之主體別名（Subject Alternative Name）

用戶憑證之主體別名（Subject Alternative Name）**應（MUST）**存在，且**應（MUST）**包含至少一個 `dNSName` 或 `iPAddress` `GeneralName`。有關可否設定之欄位及其驗證要求，詳見下文。

若憑證之 `subject` 欄位為空序列（empty SEQUENCE），本擴充欄位**應（MUST）**標記為關鍵（critical），如 RFC 5280 第 4.2.1.6 節 所規定。否則，本擴充欄位**不得（MUST NOT）**標記為關鍵（critical）。

| GeneralName 名稱類型 | 可否設定 | 驗證方法 |
| --- | --- | --- |
| otherName | N | - |
| rfc822Name | N | - |
| dNSName | Y | 該項目**應（MUST）**包含 CA 已依第 3.2.2.4 節驗證之完全吻合網域名稱（FQDN）或萬用網域名稱（Wildcard Domain Name）。萬用網域名稱**應（MUST）**依第 3.2.2.6 節進行驗證，以確認符合該節之規定。該項目**不得（MUST NOT）**包含內部名稱（Internal Name）。自 2026-03-15 起，該項目**不得（MUST NOT）**包含以 IP 位址反向區域後綴（IP Address Reverse Zone Suffix）結尾之網域名稱。該項目所含之完全吻合網域名稱（FQDN），或萬用網域名稱之 FQDN 部分，**應（MUST）**完全由 P-Labels 或非保留 LDH 標籤（Non-Reserved LDH Labels）組成，並以 U+002E FULL STOP（「.」）字元相互連接。代表網際網路網域名稱系統（DNS）根區域（root zone）之零長度網域標籤（zero-length Domain Label）**不得（MUST NOT）**包含於其中（例如，「example.com」**應（MUST）**編碼為「example.com」，而**不得（MUST NOT）**編碼為「example.com.」）。 |
| x400Address | N | - |
| directoryName | N | - |
| ediPartyName | N | - |
| uniformResourceIdentifier | N | - |
| iPAddress | Y | 該項目**應（MUST）**包含 CA 已透過第 3.2.2.5 節所規定之方法，確認申請者控管權或已獲授權使用 IPv4 或 IPv6 位址。該項目**不得（MUST NOT）**包含保留 IP 位址（Reserved IP Address）。 |
| registeredID | N | - |

subjectAltName 擴充欄位中之 GeneralName 名稱類型

**注意**：作為 RFC 5280 之明確例外，P-Labels 可不符合 IDNA 2003。本文件允許包含不符合 IDNA 2003 之 P-Labels，以支援各項 IDNA 標準之改進，包括支援較新版本之 Unicode 字元範圍（character repertoire）。

### 7.1.2.8 OCSP 回應伺服器（OCSP Responder）憑證剖繪

若簽發憑證機構（Issuing CA）不直接簽章 OCSP 回應，**得（MAY）**使用 RFC 6960 第 4.2.2.2 節 所定義之 OCSP 授權回應伺服器（OCSP Authorized Responder）。該回應伺服器的簽發憑證機構（Issuing CA of the Responder）**應（MUST）**與回應伺服器所提供的 OCSP 回應之憑證的簽發憑證機構（Issuing CA）相同。

| 欄位 | 說明 |
| --- | --- |
| `tbsCertificate` | |
| `version` | **應（MUST）**為 v3(2) |
| `serialNumber` | **應（MUST）**為一個非連續之數值，其值大於 0 且小於 $2^{159}$，且其中至少 64 個位元應來自 CSPRNG 之輸出。 |
| `signature` | 參見第 7.1.3.2 節 |
| `issuer` | **應（MUST）**與簽發憑證機構（Issuing CA）之 `subject` 欄位逐位元組完全相同。參見第 7.1.4.1 節 |
| `validity` | 參見第 7.1.2.8.1 節 |
| `subject` | 參見第 7.1.2.10.2 節 |
| `subjectPublicKeyInfo` | 參見第 7.1.3.1 節 |
| `issuerUniqueID` | **不得（MUST NOT）**存在 |
| `subjectUniqueID` | **不得（MUST NOT）**存在 |
| `extensions` | 參見第 7.1.2.8.2 節 |
| `signatureAlgorithm` | 編碼後之值**應（MUST）**與 `tbsCertificate.signature` 逐位元組完全相同 |
| `signature` | |

### 7.1.2.8.1 OCSP 回應伺服器（OCSP Responder）之有效期

| 欄位 | 最小值 | 最大值 |
| --- | --- | --- |
| `notBefore` | 簽章時間前 1 日 | 簽章時間 |
| `notAfter` | 簽章時間 | 未指定 |

### 7.1.2.8.2 OCSP 回應伺服器（OCSP Responder）之擴充欄位

| 擴充欄位 | 必要性 | 關鍵性 | 說明 |
| --- | --- | --- | --- |
| `authorityKeyIdentifier` | 應（MUST） | N | 參見第 7.1.2.11.1 節 |
| `extKeyUsage` | 應（MUST） | - | 參見第 7.1.2.8.5 節 |
| `id-pkix-ocsp-nocheck` | 應（MUST） | N | 參見第 7.1.2.8.6 節 |
| `keyUsage` | 應（MUST） | Y | 參見第 7.1.2.8.7 節 |
| `basicConstraints` | 得（MAY） | Y | 參見第 7.1.2.8.4 節 |
| `nameConstraints` | 不得（MUST NOT） | - | - |
| `subjectAltName` | 不得（MUST NOT） | - | - |
| `subjectKeyIdentifier` | 宜（SHOULD） | N | 參見第 7.1.2.11.4 節 |
| `authorityInformationAccess` | 不建議（NOT RECOMMENDED） | N | 參見第 7.1.2.8.3 節 |
| `certificatePolicies` | 不宜（SHOULD NOT） | N | 參見第 7.1.2.8.8 節 |
| `crlDistributionPoints` | 不得（MUST NOT） | N | 參見第 7.1.2.11.2 節 |
| Signed Certificate Timestamp（SCT）清單 | 得（MAY） | N | 參見第 7.1.2.11.3 節 |
| 任何其他擴充欄位 | 不建議（NOT RECOMMENDED） | - | 參見第 7.1.2.11.5 節 |

### 7.1.2.8.3 OCSP 回應伺服器（OCSP Responder）之憑證機構資訊存取（Authority Information Access）

對於 OCSP 回應伺服器憑證，本擴充欄位**不建議（NOT RECOMMENDED）**使用，因信賴憑證者（Relying Party）應已具備必要資訊。信賴憑證者須能取得簽發憑證機構（Issuing CA）之憑證，方能驗證該回應伺服器憑證，因此無需提供 `id-ad-caIssuers`。同樣地，由於 OCSP 回應伺服器憑證須包含 `id-pkix-ocsp-nocheck` 擴充欄位，信賴憑證者不會檢查此類 OCSP 回應，因此亦無需提供 `id-ad-ocsp`。

若存在，`AuthorityInfoAccessSyntax` **應（MUST）**包含一個或多個 `AccessDescription`。每個 `AccessDescription` **應（MUST）**僅包含下表所列之允許 `accessMethod`，且每個 `AuthorityInfoAccessSyntax` **應（MUST）**包含所有要求的 `AccessDescription`。

| accessMethod | accessLocation | 必要性 | 最大數量 | 說明 |
| --- | --- | --- | --- | --- |
| id-ad-ocsp（OID：1.3.6.1.5.5.7.48.1） | uniformResourceIdentifier | 不建議（NOT RECOMMENDED） | *（任意數量） | 簽發憑證機構（Issuing CA）的 OCSP 回應伺服器 HTTP URL。 |
| 任何其他值 | - | 不得（MUST NOT） | - | 不得使用其他 accessMethod。 |

#### 7.1.2.8.4 OCSP 回應伺服器（OCSP Responder）之基本限制（Basic Constraints）

OCSP 回應伺服器憑證**不得（MUST NOT）**為 CA 憑證。簽發憑證機構（issuing CA）得以下列兩種方式之一表明該憑證非 CA 憑證：不包含 basicConstraints 擴充欄位，或包含將 cA 布林值設為 FALSE 的 basicConstraints 擴充欄位。

| 欄位 | 說明 |
| --- | --- |
| cA | **應（MUST）**為 FALSE |
| pathLenConstraint | **不得（MUST NOT）**存在 |

**注意**：依 DER 對 OPTIONAL 欄位中 DEFAULT 值之編碼規則，將 cA 布林值設為 FALSE 的 basicConstraints 擴充欄位，其 extnValue OCTET STRING 內容**應（MUST）**確切為十六進位編碼之位元組 3000，即空 ASN.1 SEQUENCE 值之編碼表示。

#### 7.1.2.8.5 OCSP 回應伺服器（OCSP Responder）之擴充金鑰使用方法（Extended Key Usage）

| 金鑰適用目的（Key Purpose） | OID | 必要性 |
| --- | --- | --- |
| id-kp-OCSPSigning | 1.3.6.1.5.5.7.3.9 | 應（MUST） |
| 任何其他值 | - | 不得（MUST NOT） |

#### 7.1.2.8.6 OCSP 回應伺服器（OCSP Responder）之 id-pkix-ocsp-nocheck

憑證機構（CA）**應（MUST）**於 OCSP 回應伺服器憑證中包含 id-pkix-ocsp-nocheck 擴充欄位（OID：1.3.6.1.5.5.7.48.1.5）。

本擴充欄位之 extnValue OCTET STRING 內容**應（MUST）**確切為十六進位編碼之位元組 0500，即 ASN.1 NULL 值之編碼表示，如 RFC 6960 第 4.2.2.2.1 節 所規定。

### 7.1.2.8.7 OCSP 回應伺服器（OCSP Responder）之憑證金鑰用途（Key Usage）

| 憑證金鑰用途（Key Usage） | 可否設定 | 設定必要性 |
|---|---|---|
| `digitalSignature` | Y | Y |
| `nonRepudiation` | N | — |
| `keyEncipherment` | N | — |
| `dataEncipherment` | N | — |
| `keyAgreement` | N | — |
| `keyCertSign` | N | — |
| `cRLSign` | N | — |
| `encipherOnly` | N | — |
| `decipherOnly` | N | — |

### 7.1.2.8.8 OCSP 回應伺服器（OCSP Responder）之憑證原則（Certificate Policies）

若存在，憑證原則（Certificate Policies）擴充欄位**應（MUST）**包含至少一個 `PolicyInformation`。每個 `PolicyInformation` **應（MUST）**符合下列剖繪：

| 欄位 | 必要性 | 內容 |
|---|---|---|
| `policyIdentifier` | 應（MUST） | 下列政策識別碼之一： |
| 保留憑證政策識別碼 | 不建議（NOT RECOMMENDED） | |
| `anyPolicy` | 不建議（NOT RECOMMENDED） | |
| 任何其他識別碼 | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**由 CA 定義，並載明於其憑證政策（CP）及／或憑證實務作業基準（CPS）中。 |
| `policyQualifiers` | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**僅包含下表所列之允許 `policyQualifiers`。 |

| Qualifier ID | 必要性 | 欄位型別 | 內容 |
| --- | --- | --- | --- |
| `id-qt-cps`（OID：1.3.6.1.5.5.7.2.1） | 得（MAY） | `IA5String` | 簽發憑證機構（Issuing CA）之憑證政策（CP）、憑證實務作業基準（CPS）、信賴憑證者協議（Relying Party Agreement），或其他由簽發憑證機構提供的線上政策資訊之 HTTP 或 HTTPS URL。 |
| 任何其他 qualifier | 不得（MUST NOT） | - | - |

允許之 `policyQualifiers`

**注意**：由於憑證原則擴充欄位可用於限制憑證的適用用途，若憑證原則設定不正確，可能導致 OCSP 回應伺服器憑證無法通過驗證，進而造成 OCSP 回應無效。包含 `anyPolicy` 政策識別碼可降低此風險，但會增加用戶端處理的複雜度，並可能造成交互運作問題。

### 7.1.2.9 預簽憑證（Precertificate）剖繪

預簽憑證（Precertificate）係一種經簽章之資料結構，如 RFC 6962 所定義，可提出至憑證透明度（Certificate Transparency）記錄系統。預簽憑證在結構上與有效憑證相同，惟其 `extensions` 欄位中包含一特殊之關鍵性 poison 擴充欄位，其 OID 為 1.3.6.1.4.1.11129.2.4.3。此擴充欄位可確保遵循 RFC 5280 之用戶端不會將預簽憑證接受為有效憑證。經簽章之預簽憑證的存在，可視為相對應有效憑證亦存在之證據，因該簽章代表 CA 對可能簽發此憑證做出具有約束力之承諾。

預簽憑證是於 CA 決定簽發憑證之後，但在實際簽章該有效憑證之前建立。CA **得（MAY）**建構並簽章與該有效憑證相對應之預簽憑證，以提出至憑證透明度記錄系統。CA **得（MAY）**使用所回傳之已簽章憑證時間戳記（Signed Certificate Timestamps，SCT），於簽章該有效憑證之前修改憑證之 `extensions` 欄位，新增如第 7.1.2.11.3 節所定義且為相關剖繪所允許之已簽章憑證時間戳記（SCT）清單。

預簽憑證一經簽章，信賴憑證者可將其視為 CA 對其簽發相對應有效憑證之意圖所做出的具有約束力之承諾，或更常見的是，視為相對應有效憑證已存在。有效憑證是否與預簽憑證相對應，是依據經 RFC 6962 第 3.2 節 所定義之流程轉換後的 `tbsCertificate` 內容值判定。

本剖繪描述將憑證轉換為預簽憑證時，所允許之轉換。CA **不得（MUST NOT）**簽發預簽憑證，除非其願意簽發相對應有效憑證，無論其是否已簽發該相對應有效憑證。同樣地，CA **不得（MUST NOT）**簽發預簽憑證，除非相對應有效憑證遵循本《基本要求》規定，無論 CA 是否簽章該相對應有效憑證。

預簽憑證可直接由簽發憑證機構（Issuing CA）簽發；若預簽憑證是於 2026-03-15 之前簽發，亦可由第 7.1.2.4 節所定義的受技術約束之預簽憑證簽章憑證機構（Signing CA）簽發。若預簽憑證是由預簽憑證簽章憑證機構簽發，則除預簽憑證 poison 擴充欄位及已簽章憑證時間戳記清單（SCT 清單）擴充欄位外，預簽憑證之 issuer 欄位及 `authorityKeyIdentifier` 擴充欄位（若存在）亦可與有效憑證不同，如下所述。

| 欄位 | 說明 |
| --- | --- |
| tbsCertificate | |
| version | 編碼後之值**應（MUST）**與有效憑證之 version 欄位逐位元組完全相同 |
| serialNumber | 編碼後之值**應（MUST）**與有效憑證之 serialNumber 欄位逐位元組完全相同 |
| signature | 編碼後之值**應（MUST）**與有效憑證之 signature 欄位逐位元組完全相同 |
| issuer | 編碼後之值**應（MUST）**與有效憑證之 issuer 欄位逐位元組完全相同 |
| validity | 編碼後之值**應（MUST）**與有效憑證之 validity 欄位逐位元組完全相同 |
| subject | 編碼後之值**應（MUST）**與有效憑證之 subject 欄位逐位元組完全相同 |
| subjectPublicKeyInfo | 編碼後之值**應（MUST）**與有效憑證之 subjectPublicKeyInfo 欄位逐位元組完全相同 |
| issuerUniqueID | 編碼後之值**應（MUST）**與有效憑證之 issuerUniqueID 欄位逐位元組完全相同，若有效憑證省略此欄位，則亦予以省略。 |
| subjectUniqueID | 編碼後之值**應（MUST）**與有效憑證之 subjectUniqueID 欄位逐位元組完全相同，若有效憑證省略此欄位，則亦予以省略。 |
| extensions | 參見第 7.1.2.9.1 節 |
| signatureAlgorithm | 編碼後之值**應（MUST）**與 tbsCertificate.signature 逐位元組完全相同 |
| signature | |

預簽憑證由簽發憑證機構（Issuing CA）直接簽發時

| 欄位 | 說明 |
| --- | --- |
| tbsCertificate | |
| version | 編碼後之值**應（MUST）**與有效憑證之 version 欄位逐位元組完全相同 |
| serialNumber | 編碼後之值**應（MUST）**與有效憑證之 serialNumber 欄位逐位元組完全相同 |
| signature | 編碼後之值**應（MUST）**與有效憑證之 signature 欄位逐位元組完全相同 |
| issuer | 編碼後之值**應（MUST）**與預簽憑證簽章憑證機構憑證之 subject 欄位逐位元組完全相同 |
| validity | 編碼後之值**應（MUST）**與有效憑證之 validity 欄位逐位元組完全相同 |
| subject | 編碼後之值**應（MUST）**與有效憑證之 subject 欄位逐位元組完全相同 |
| subjectPublicKeyInfo | 編碼後之值**應（MUST）**與有效憑證之 subjectPublicKeyInfo 欄位逐位元組完全相同 |
| issuerUniqueID | 編碼後之值**應（MUST）**與有效憑證之 issuerUniqueID 欄位逐位元組完全相同，若有效憑證省略此欄位，則亦予以省略。 |
| subjectUniqueID | 編碼後之值**應（MUST）**與有效憑證之 subjectUniqueID 欄位逐位元組完全相同，若有效憑證省略此欄位，則亦予以省略。 |
| extensions | 參見第 7.1.2.9.2 節 |
| signatureAlgorithm | 編碼後之值**應（MUST）**與 tbsCertificate.signature 逐位元組完全相同 |
| signature | |

預簽憑證由預簽憑證簽章憑證機構（Precertificate Signing CA）代簽發憑證機構（Issuing CA）簽發時

**注意**：本剖繪要求預簽憑證之 serialNumber 欄位與相對應有效憑證之 serialNumber 欄位完全相同。RFC 5280 第 4.1.2.2 節 要求憑證之 serialNumber 必須具唯一性。就本文件而言，預簽憑證不應被視為受該 RFC 要求規範之「憑證」，因此得與相對應有效憑證具有相同之 serialNumber。然而，除非兩個預簽憑證對應於同一有效憑證，否則不得共用相同之 serialNumber，因為此情形將表示存在兩個具有相同 serialNumber 之相對應有效憑證。

### 7.1.2.9.1 預簽憑證（Precertificate）剖繪之擴充欄位－直接簽發（Directly Issued）

這些擴充欄位適用於由 CA 直接簽發之預簽憑證，而不適用於使用第 7.1.2.4 節所定義之預簽憑證簽章憑證機構（Precertificate Signing CA）憑證所簽發之預簽憑證。

| 擴充欄位 | 必要性 | 關鍵性 | 說明 |
| --- | --- | --- | --- |
| Precertificate Poison（OID：1.3.6.1.4.1.11129.2.4.3） | 應（MUST） | Y | 參見第 7.1.2.9.3 節 |
| Signed Certificate Timestamp（SCT）清單 | 不得（MUST NOT） | - | |
| 任何其他擴充欄位 | * | * | 所有其他擴充欄位之順序、關鍵性及編碼後之值**應（MUST）**與有效憑證之 `extensions` 欄位逐位元組完全相同。 |

**注意**：本項要求係指：若自預簽憑證中移除 Precertificate Poison 擴充欄位，並自有效憑證中移除 Signed Certificate Timestamp（SCT）清單擴充欄位，則預簽憑證之 `extensions` 欄位內容與有效憑證之 `extensions` 欄位內容**應（MUST）**逐位元組完全相同。

### 7.1.2.9.2 預簽憑證（Precertificate）剖繪之擴充欄位－預簽憑證憑證機構簽發（Precertificate CA Issued）

這些擴充欄位適用於使用第 7.1.2.4 節所定義之預簽憑證簽章憑證機構（Precertificate Signing CA）憑證所簽發之預簽憑證。對於此類預簽憑證，若有效憑證中存在 `authorityKeyIdentifier`，則預簽憑證中的 `authorityKeyIdentifier` 會依 RFC 6962 第 3.2 節 所述予以修改。

| 擴充欄位 | 必要性 | 關鍵性 | 說明 |
| --- | --- | --- | --- |
| Precertificate Poison（OID：1.3.6.1.4.1.11129.2.4.3） | 應（MUST） | Y | 參見第 7.1.2.9.3 節 |
| `authorityKeyIdentifier` | * | * | 參見第 7.1.2.9.4 節 |
| Signed Certificate Timestamp（SCT）清單 | 不得（MUST NOT） | - | |
| 任何其他擴充欄位 | * | * | 所有其他擴充欄位之順序、關鍵性及編碼後之值**應（MUST）**與有效憑證之 `extensions` 欄位逐位元組完全相同。 |

### 7.1.2.9.3 預簽憑證（Precertificate）Poison

預簽憑證**應（MUST）**包含 Precertificate Poison 擴充欄位（OID：1.3.6.1.4.1.11129.2.4.3）。

本擴充欄位之 `extnValue OCTET STRING` 內容**應（MUST）**確切為十六進位編碼之位元組 `0500`，即 ASN.1 `NULL` 值之編碼表示，如 RFC 6962 第 3.1 節 所規定。

### 7.1.2.9.4 預簽憑證（Precertificate）之授權單位金鑰識別碼（Authority Key Identifier）

對於由預簽憑證簽章憑證機構（Precertificate Signing CA）所簽發之預簽憑證，`authorityKeyIdentifier` 擴充欄位之內容**應（MUST）**符合下列任一情形：

1. **宜（SHOULD）**依下表之剖繪設定；或
2. **得（MAY）**與相對應憑證之 `authorityKeyIdentifier` 擴充欄位內容逐位元組完全相同。

| 欄位 | 說明 |
| --- | --- |
| `keyIdentifier` | **應（MUST）**存在。**應（MUST）**與預簽憑證簽章憑證機構憑證之 `subjectKeyIdentifier` 欄位完全相同 |
| `authorityCertIssuer` | **不得（MUST NOT）**存在 |
| `authorityCertSerialNumber` | **不得（MUST NOT）**存在 |

**注意**：RFC 6962 描述如何轉換預簽憑證中的 `authorityKeyIdentifier`，使其包含預簽憑證簽章憑證機構的 `authorityKeyIdentifier` 擴充欄位值（即反映實際簽發者憑證的 `keyIdentifier`），從而使其在用戶端驗證時與相對應有效憑證相符。本《基本要求》**建議（RECOMMENDED）**由預簽憑證簽章憑證機構簽發之預簽憑證，其 `authorityKeyIdentifier` 使用該簽章憑證機構之 `authorityKeyIdentifier` 擴充欄位中的 `keyIdentifier`，以確保憑證鏈中所有憑證之 `subjectKeyIdentifier` 與 `authorityKeyIdentifier` 具有一致性。雖然 RFC 5280 並未嚴格要求此種一致性，但已有若干用戶端實作會對憑證強制執行此種一致性檢查，而採用上述作法可避免因憑證透明度記錄系統（Certificate Transparency Log）錯誤實作此類檢查而產生的風險。

#### 7.1.2.10 憑證機構（CA）共通欄位

本節列出多個憑證機構（Certification Authority，CA）憑證剖繪所共通之若干欄位。然而，這些欄位未必為所有 CA 憑證剖繪所共通。於簽發憑證之前，CA **應（MUST）**確保整張憑證的內容（包括各欄位之內容）均遵循第 7.1.2 節所載明之至少一個憑證剖繪的所有要求。

#### 7.1.2.10.1 憑證機構（CA）憑證之有效期

| 欄位 | 最小值 | 最大值 |
| --- | --- | --- |
| `notBefore` | 簽章時間前 1 日 | 簽章時間 |
| `notAfter` | 簽章時間 | 未指定 |

#### 7.1.2.10.2 憑證機構（CA）憑證之填名（Naming）

所有 `subject` 名稱**應（MUST）**依第 7.1.4 節規定之方式編碼。

下表列出 `AttributeTypeAndValue` 之 `type` 欄位允許使用的 `AttributeType`，以及對應之 `value` 欄位允許填列的內容。

| AttributeType 屬性名稱 | 必要性 | value | 驗證方法 |
| --- | --- | --- | --- |
| countryName | 應（MUST） | 為 CA 營業所在地國家之兩字母 ISO 3166-1 國家代碼。 | 第 3.2.2.3 節 |
| stateOrProvinceName | 得（MAY） | 若存在，為 CA 營業所在地之州或省份資訊。 | 第 3.2.2.1 節 |
| localityName | 得（MAY） | 若存在，為 CA 營業所在地之縣市地區資訊。 | 第 3.2.2.1 節 |
| postalCode | 得（MAY） | 若存在，為 CA 營業所在地之郵遞區號資訊。 | 第 3.2.2.1 節 |
| streetAddress | 得（MAY） | 若存在，為 CA 營業所在地之街道地址資訊。**得（MAY）**包含多個實體地址。 | 第 3.2.2.1 節 |
| organizationName | 應（MUST） | 為 CA 之名稱或商業名稱（DBA）。CA **得（MAY）**在此欄位包含與已驗證名稱略有出入之資訊，例如常見之變體或縮寫，前提是 CA 須以書面文件記錄其差異及所使用之縮寫為當地公認之縮寫；例如：若官方記錄顯示為「Company Name Incorporated」，CA **得（MAY）**使用「Company Name Inc.」或「Company Name」。 | 第 3.2.2.2 節 |
| organizationalUnitName | 第 7.1.2.1 節所定義之根憑證機構憑證、第 7.1.2.5 節所定義之 TLS 下屬憑證機構憑證，或第 7.1.2.6 節所定義之受技術約束之 TLS 下屬憑證機構憑證**不得（MUST NOT）**包含此屬性。其他類型之 CA 憑證**不宜（SHOULD NOT）**包含此屬性。 | - | - |
| commonName | 應（MUST） | 其內容**宜（SHOULD）**作為該憑證之識別資訊，以確保該憑證 Name 在同一簽發者所簽發之所有憑證中具有唯一性。 | |
| 任何其他屬性 | 不建議（NOT RECOMMENDED） | - | 參見第 7.1.4.4 節 |

#### 7.1.2.10.3 憑證機構（CA）憑證之憑證機構資訊存取（Authority Information Access）

若存在，`AuthorityInfoAccessSyntax` **應（MUST）**包含一個或多個 `AccessDescription`。每個 `AccessDescription` **應（MUST）**僅包含下表所列之允許 `accessMethod`，且每個 `accessLocation` **應（MUST）**編碼為指定之 `GeneralName` 型別。

若該 `accessMethod` 允許指定多個 `AccessDescription`，`AuthorityInfoAccessSyntax` **得（MAY）**包含多個具有相同 `accessMethod` 的 `AccessDescription`。當存在多個具有相同 `accessMethod` 的 `AccessDescription` 時，各 `accessLocation` **應（MUST）**互不相同，且各 `AccessDescription` **應（MUST）**依該 `accessMethod` 之優先順位排列，其中具有最高優先順位 `accessLocation` 的 `AccessDescription` 應排列於首位。在符合前述要求之前提下，對於具有不同 `accessMethod` 的 `AccessDescription`，不另定其排序要求。

| accessMethod | accessLocation | 必要性 | 最大數量 | 說明 |
|---|---|---|---|---|
| `id-ad-ocsp`（OID：1.3.6.1.5.5.7.48.1） | `uniformResourceIdentifier` | 得（MAY） | *（任意數量） | 簽發憑證機構（Issuing CA）的 OCSP 回應伺服器 HTTP URL。 |
| `id-ad-caIssuers`（OID：1.3.6.1.5.5.7.48.2） | `uniformResourceIdentifier` | 得（MAY） | *（任意數量） | 簽發憑證機構憑證的 HTTP URL。 |
| 任何其他值 | - | 不得（MUST NOT） | - | 不得使用其他 `accessMethod`。 |

#### 7.1.2.10.4 憑證機構（CA）憑證之基本限制（Basic Constraints）

| 欄位 | 說明 |
|---|---|
| `cA` | **應（MUST）**設為 TRUE |
| `pathLenConstraint` | **得（MAY）**存在 |

#### 7.1.2.10.5 憑證機構（CA）憑證之憑證原則（Certificate Policies）

若存在，憑證原則（Certificate Policies）擴充欄位**應（MUST）**包含至少一個 `PolicyInformation`。每個 `PolicyInformation` **應（MUST）**符合下列剖繪：

| 欄位 | 必要性 | 內容 |
| --- | --- | --- |
| `policyIdentifier` | 應（MUST） | 當簽發憑證機構（Issuing CA）欲表示不存在何政策限制，且下屬憑證機構（Subordinate CA）為其關係企業時，簽發憑證機構**得（MAY）**使用 `anyPolicy` 政策識別碼；此時，憑證原則擴充欄位中**應（MUST）**僅包含此一 `PolicyInformation` 值。 |
| `anyPolicy` | 應（MUST） | |
| `policyQualifiers` | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**僅包含下表所列之允許 `policyQualifiers`。 |

無政策限制（適用於關係企業 CA）

| 欄位 | 必要性 | 內容 |
| --- | --- | --- |
| `policyIdentifier` | 應（MUST） | 下列政策識別碼之一： |
| 保留憑證政策識別碼 | 應（MUST） | CA **應（MUST）**包含僅有一個保留憑證政策識別碼（參見第 7.1.6.1 節），以對應由本憑證所代表之 CA 直接或間接簽發之指定用戶憑證類型（參見第 7.1.2.7.1 節）。 |
| `anyPolicy` | 不得（MUST NOT） | `anyPolicy` 政策識別碼**不得（MUST NOT）**存在。 |
| 任何其他識別碼 | 得（MAY） | 若存在，**應（MUST）**由 CA 定義，並載明於其憑證政策（CP）及／或憑證實務作業基準（CPS）中。 |
| `policyQualifiers` | 不建議（NOT RECOMMENDED） | 若存在，**應（MUST）**僅包含下表所列之允許 `policyQualifiers`。 |

受政策限制

受政策限制剖繪**建議（RECOMMENDED）**憑證原則擴充欄位中之第一個 `PolicyInformation` 值包含保留憑證政策識別碼（參見第 7.1.6.1 節）[3]。無論 `PolicyInformation` 值之順序為何，憑證原則擴充欄位**應（MUST）**包含僅有一個保留憑證政策識別碼。

**注意**：依本憑證剖繪簽發之任何憑證均**不建議（NOT RECOMMENDED）**包含 `policyQualifiers`，因為此資訊會增加憑證大小，但對一般信賴憑證者並無實質價值，且於必要時可透過其他方式取得。

若允許使用 `policyQualifiers`，且其存在於 `PolicyInformation` 欄位中，**應（MUST）**依下列格式編排：

| Qualifier ID | 必要性 | 欄位型別 | 內容 |
| --- | --- | --- | --- |
| `id-qt-cps`（OID：1.3.6.1.5.5.7.2.1） | 得（MAY） | `IA5String` | 簽發憑證機構（Issuing CA）之憑證政策（CP）、憑證實務作業基準（CPS）、信賴憑證者協議（Relying Party Agreement），或其他由簽發憑證機構提供的線上政策資訊之 HTTP 或 HTTPS URL。 |
| 任何其他 qualifier | 不得（MUST NOT） | - | - |

允許之 `policyQualifiers`

### 7.1.2.10.6 憑證機構（CA）憑證之擴充金鑰使用方法（Extended Key Usage）

| 金鑰適用目的（Key Purpose） | OID | 必要性 |
| --- | --- | --- |
| `id-kp-serverAuth` | 1.3.6.1.5.5.7.3.1 | 應（MUST） |
| `id-kp-clientAuth` | 1.3.6.1.5.5.7.3.2 | 得（MAY） |
| `id-kp-codeSigning` | 1.3.6.1.5.5.7.3.3 | 不得（MUST NOT） |
| `id-kp-emailProtection` | 1.3.6.1.5.5.7.3.4 | 不得（MUST NOT） |
| `id-kp-timeStamping` | 1.3.6.1.5.5.7.3.8 | 不得（MUST NOT） |
| `id-kp-OCSPSigning` | 1.3.6.1.5.5.7.3.9 | 不得（MUST NOT） |
| `anyExtendedKeyUsage` | 2.5.29.37.0 | 不得（MUST NOT） |
| 預簽憑證簽章憑證 | 1.3.6.1.4.1.11129.2.4.4 | 不得（MUST NOT） |
| 任何其他值 | - | 不建議（NOT RECOMMENDED） |

### 7.1.2.10.7 憑證機構（CA）憑證之憑證金鑰用途（Key Usage）

| 憑證金鑰用途（Key Usage） | 可否設定 | 設定必要性 |
|---|---|---|
| digitalSignature | Y | N[4] |
| nonRepudiation | N | — |
| keyEncipherment | N | — |
| dataEncipherment | N | — |
| keyAgreement | N | — |
| keyCertSign | Y | Y |
| cRLSign | Y | Y |
| encipherOnly | N | — |
| decipherOnly | N | — |

### 7.1.2.10.8 憑證機構（CA）憑證之名稱限制（Name Constraints）

若存在，名稱限制（Name Constraints）擴充欄位**應（MUST）**依下列方式編碼。作為 RFC 5280 之明確例外，本擴充欄位**宜（SHOULD）**標記為關鍵（critical），但若需與某些不支援名稱限制之舊版應用程式相容，**得（MAY）**標記為非關鍵（non-critical）。

| 欄位 | 說明 |
|---|---|
| permittedSubtrees | |
| GeneralSubtree | 符合 permittedSubtrees 中各 GeneralSubtree 之要求規定 |
| base | 參見下表 |
| minimum | **不得（MUST NOT）**存在 |
| maximum | **不得（MUST NOT）**存在 |
| excludedSubtrees | |
| GeneralSubtree | 符合 permittedSubtrees 中各 GeneralSubtree 之要求規定 |
| base | 參見下表 |
| minimum | **不得（MUST NOT）**存在 |
| maximum | **不得（MUST NOT）**存在 |

nameConstraints 要求規定

下表列出 permittedSubtrees 或 excludedSubtrees 中各 GeneralSubtree 之 base 所包含的 GeneralName 要求規定。

| GeneralName 名稱類型 | 必要性 | permittedSubtrees | excludedSubtrees |
|---|---|---|---|
| dNSName | 得（MAY） | CA **應（MUST）**確認申請者已註冊該 dNSName，或已獲網域名稱註冊人授權代表該註冊人行事。參見第 3.2.2.4 節。 | 若 permittedSubtrees 中至少存在一個 dNSName，CA **得（MAY）**於 excludedSubtrees 指定 dNSName 網域之一個或多個子網域名稱作為欲排除項目。 |
| iPAddress | 得（MAY） | CA **應（MUST）**確認申請者已被指配該 iPAddress 範圍，或已獲 IP 位址分配者（assigner）授權代表被指配者（assignee）行事。參見第 3.2.2.5 節。 | 若 permittedSubtrees 中至少存在一個 iPAddress，CA **得（MAY）**於 excludedSubtrees 指定該等 iPAddress 範圍內之一個或多個子網段作為欲排除項目。 |
| directoryName | 得（MAY） | CA **應（MUST）**確認申請者及／或其子公司之名稱屬性，以確保所有簽發之憑證均遵循相關憑證剖繪（參見第 7.1.2 節），包括名稱形式（參見第 7.1.4 節）之要求。 | 不建議（NOT RECOMMENDED）於 excludedSubtrees 中包含任何值。 |
| rfc822Name | 不建議（NOT RECOMMENDED） | CA **得（MAY）**將其限制為信箱、特定主機或網域內之任何網址，如 RFC 5280 第 4.2.1.10 節所規定。對於每個主機、網域或信箱之網域部分（如 RFC 5280 第 4.2.1.6 節所規定），CA **應（MUST）**確認申請者已註冊該網域，或已獲網域名稱註冊人授權代表該註冊人行事。參見第 3.2.2.4 節。 | 若 permittedSubtrees 中至少存在一個 rfc822Name，CA **得（MAY）**於 excludedSubtrees 指定一個或多個信箱、主機或網域作為欲排除項目。 |
| otherName | 不建議（NOT RECOMMENDED） | 參見下文 | 參見下文 |
| 任何其他值 | 不建議（NOT RECOMMENDED） | - | - |

base 欄位所包含之 GeneralName 要求規定

任何 otherName，若存在：

1. **應（MUST）**適用於公共網際網路，除非：

a. `type-id` 位於申請者能證明擁有其所有權之 OID arc 範圍內，或

b. 申請者能以其他方式證明其有權於公共網際網路中聲明該資料。

2. **不得（MUST NOT）**具有可能使信賴憑證者對 CA 所驗證之憑證資訊產生誤解的含義。
3. **應（MUST）**依相關 ASN.1 模組中對該 `otherName` 的 `type-id` 與 `value` 之定義，以 DER 進行編碼。

CA **不得（SHALL NOT）**包含額外名稱（例如額外的 `GeneralName`），除非 CA 知悉有正當理由於憑證中包含該資料。

#### 7.1.2.11 憑證共通欄位

本節列出多個憑證剖繪所共通之若干欄位。然而，這些欄位未必為所有憑證剖繪所共通。於簽發憑證之前，憑證機構（Certification Authority，CA）**應（MUST）**確保整張憑證的內容（包括各欄位之內容）均遵循第 7.1.2 節所載明之至少一個憑證剖繪的所有要求。

##### 7.1.2.11.1 授權單位金鑰識別碼（Authority Key Identifier）

| 欄位 | 說明 |
| --- | --- |
| `keyIdentifier` | **應（MUST）**存在。**應（MUST）**與簽發憑證機構（Issuing CA）之 `subjectKeyIdentifier` 欄位完全相同 |
| `authorityCertIssuer` | **不得（MUST NOT）**存在 |
| `authorityCertSerialNumber` | **不得（MUST NOT）**存在 |

##### 7.1.2.11.2 CRL 發布點

CRL 發布點（CRL Distribution Points）擴充欄位**應（MUST）**存在於：

- 下屬憑證機構（Subordinate CA）憑證；及
- （1）不符合「短效期用戶憑證」資格，且（2）未包含具有 `id-ad-ocsp` accessMethod 之憑證機構資訊存取（AIA）擴充欄位的用戶憑證。

CRL 發布點擴充欄位**不宜（SHOULD NOT）**存在於：

- 根憑證機構（Root CA）憑證。

CRL 發布點擴充欄位於以下情況為**選用（OPTIONAL）**：

- 短效期用戶憑證（Short-lived Subscriber Certificates）。

CRL 發布點擴充欄位**不得（MUST NOT）**存在於：

- OCSP 回應伺服器（OCSP Responder）憑證。

若存在，CRL 發布點擴充欄位**應（MUST）**包含至少一個 `DistributionPoint`；若包含超過一個，則**不建議（NOT RECOMMENDED）**。所有 `DistributionPoint` 應依下列格式編排：

| 欄位 | 必要性 | 說明 |
|---|---|---|
| `distributionPoint` | 應（MUST） | `DistributionPointName` **應（MUST）**為 `fullName`，格式如下所述。 |
| `reasons` | 不得（MUST NOT） | |
| `cRLIssuer` | 不得（MUST NOT） | |

`DistributionPoint` 剖繪

`fullName` **應（MUST）**包含至少一個 `GeneralName`；**得（MAY）**包含超過一個。所有 `GeneralName` **應（MUST）**為 `uniformResourceIdentifier` 類型，且每個 scheme **應（MUST）**為「http」。第一個 `GeneralName` 應包含本憑證之簽發憑證機構（Issuing CA）所提供之 CRL 服務的 HTTP URL。

#### 7.1.2.11.3 已簽章憑證時間戳記（SCT）清單

若存在，SCT 清單（Signed Certificate Timestamp List）擴充欄位之內容**應（MUST）**為一個 `OCTET STRING`，其中包含依 RFC 6962 第 3.3 節 規定編碼之 `SignedCertificateTimestampList`。

`SignedCertificateTimestampList` 中所包含的每個 `SignedCertificateTimestamp` **應（MUST）**係針對其所對應之當前憑證的 `PreCert` `LogEntryType`（precert_entry 類型）而簽發。

#### 7.1.2.11.4 主體金鑰識別碼（Subject Key Identifier）

若存在，`subjectKeyIdentifier` **應（MUST）**依 RFC 5280 第 4.2.1.2 節 所定義之方式設定。CA **應（MUST）**針對每個唯一公開金鑰（即 `tbsCertificate` 的 `subjectPublicKeyInfo` 欄位），產生一個於其所有已簽發憑證中均唯一之 `subjectKeyIdentifier`。例如，CA 可使用以公開金鑰為輸入之演算法產生 `subjectKeyIdentifier`，或可使用 CSPRNG（密碼學安全偽亂數產生器）產生一個足夠大之唯一數值。

#### 7.1.2.11.5 其他擴充欄位

所有適用之憑證剖繪未直接規範的擴充欄位及擴充欄位值：

1. **應（MUST）**適用於公共網際網路，除非：
   a. 擴充欄位 OID 位於申請者能證明擁有其所有權之 OID arc 範圍內，或
   b. 申請者能以其他方式證明其有權於公共網際網路中聲明該資料。
2. **不得（MUST NOT）**具有可能使信賴憑證者對 CA 所驗證之憑證資訊產生誤解的含義（例如，憑證包含表示私密金鑰儲存於智慧卡之擴充欄位，而 CA 因採行遠端簽發，無法驗證對應之私密金鑰是否確實僅存在於該硬體內）。
3. **應（MUST）**依相關 ASN.1 模組中對該擴充欄位及擴充欄位值之定義，以 DER 編碼。

CA **不得（SHALL NOT）**包含額外擴充欄位或欄位值，除非 CA 知悉有正當理由於憑證中包含該資料。

### 7.1.3 演算法物件識別碼

#### 7.1.3.1 主體公開金鑰資訊（SubjectPublicKeyInfo）

下列要求適用於有效憑證或預簽憑證中的 `subjectPublicKeyInfo` 欄位。不得使用其他編碼方式。

##### 7.1.3.1.1 RSA

CA **應（SHALL）**使用 `rsaEncryption`（OID：1.2.840.113549.1.1.1）演算法識別碼表示 RSA 金鑰。參數**應（MUST）**存在，且**應（MUST）**為明確的 NULL。 CA **不得（SHALL NOT）**使用其他演算法（例如 `id-RSASSA-PSS`（OID：1.2.840.113549.1.1.10）演算法識別碼）表示 RSA 金鑰。

編碼時，RSA 金鑰的 `AlgorithmIdentifier` **應（MUST）**與下列十六進位編碼位元組逐位元組完全相同：`300d06092a864886f70d0101010500`

##### 7.1.3.1.2 ECDSA

CA **應（SHALL）**使用 `id-ecPublicKey`（OID：1.2.840.10045.2.1）演算法識別碼表示 ECDSA 金鑰。參數**應（MUST）**使用 `namedCurve` 編碼方式。

- P-256 金鑰之 `namedCurve` **應（MUST）**為 `secp256r1`（OID：1.2.840.10045.3.1.7）。
- P-384 金鑰之 `namedCurve` **應（MUST）**為 `secp384r1`（OID：1.3.132.0.34）。
- P-521 金鑰之 `namedCurve` **應（MUST）**為 `secp521r1`（OID：1.3.132.0.35）。

編碼時，ECDSA 金鑰的 `AlgorithmIdentifier` **應（MUST）**與下列十六進位編碼位元組逐位元組完全相同：

- P-256 金鑰：`301306072a8648ce3d020106082a8648ce3d030107`。
- P-384 金鑰：`301006072a8648ce3d020106052b81040022`。
- P-521 金鑰：`301006072a8648ce3d020106052b81040023`。

#### 7.1.3.2 簽章演算法識別碼（Signature AlgorithmIdentifier）

所有使用 CA 私密金鑰（Private Key）簽章之物件，**應（MUST）**符合本節有關 `AlgorithmIdentifier` 或 `AlgorithmIdentifier` 衍生型別於簽章情境下使用的要求規定。

具體而言，本節要求規定適用於下列所有物件及欄位：

- 有效憑證或預簽憑證的 `signatureAlgorithm` 欄位。
- TBSCertificate 的 `signature` 欄位（例如有效憑證或預簽憑證所使用的 TBSCertificate）。
- CertificateList 的 `signatureAlgorithm` 欄位。
- TBSCertList 的 `signature` 欄位。
- BasicOCSPResponse 的 `signatureAlgorithm` 欄位。

上述欄位不得使用其他編碼方式。

#### 7.1.3.2.1 RSA

CA **應（SHALL）**使用下列簽章演算法及編碼之一。編碼時，`AlgorithmIdentifier` **應（MUST）**與指定的十六進位編碼位元組逐位元組完全相同。

- 採用 SHA-256 的 RSASSA-PKCS1-v1_5：

  編碼：`300d06092a864886f70d01010b0500`。

- 採用 SHA-384 的 RSASSA-PKCS1-v1_5：

  編碼：`300d06092a864886f70d01010c0500`。

- 採用 SHA-512 的 RSASSA-PKCS1-v1_5：

  編碼：`300d06092a864886f70d01010d0500`。

- 採用 SHA-256 的 RSASSA-PSS、採用 SHA-256 的 MGF-1，以及 32 位元組的鹽值長度：

  編碼：

  ```
  HEXDUMP

  304106092a864886f70d01010a3034a00f300d060960864801650304020 1
  0500a11c301a06092a864886f70d010108300d060960864801650304020 1
  0500a203020120
  ```

- 採用 SHA-384 的 RSASSA-PSS、採用 SHA-384 的 MGF-1，以及 48 位元組的鹽值長度：

  編碼：

  ```
  HEXDUMP

  304106092a864886f70d01010a3034a00f300d060960864801650304020 2
  0500a11c301a06092a864886f70d010108300d060960864801650304020 2
  0500a203020130
  ```

- 採用 SHA-512 的 RSASSA-PSS、採用 SHA-512 的 MGF-1，以及 64 位元組的鹽值長度：

  編碼：

  ```
  HEXDUMP

  304106092a864886f70d01010a3034a00f300d060960864801650304020 3
  0500a11c301a06092a864886f70d010108300d060960864801650304020 3
  0500a203020140
  ```

於 2026-09-15 之前，若符合下列所有條件，CA **得（MAY）**使用下列 SHA-1 簽章演算法及編碼：

- 若用於憑證（例如憑證的 `signatureAlgorithm` 欄位或 TBSCertificate 的 `signature` 欄位）：

- 新憑證為根憑證機構（Root CA）憑證，或屬於交互認證（Cross-Certificate）之下屬憑證機構（Subordinate CA）憑證；且，
- 存在一張由相同簽發憑證機構憑證（issuing CA Certificate）所簽發，且簽章演算法使用下列 SHA-1 編碼的現有憑證；且，
- 該現有憑證的 `serialNumber` 長度至少為 64 位元；且，
- 新憑證與現有憑證之間的差異僅限於下列一項或多項：
  - `subjectPublicKeyInfo` 中有一個新的 `subjectPublicKey`，且使用相同的演算法與金鑰長度；及／或，
  - 有一個新的 `serialNumber`，其編碼長度與現有憑證相同；及／或，
  - 新憑證的 `extKeyUsage` 擴充欄位存在、至少指定一種金鑰適用目的（key purpose），且所指定之金鑰適用目的均非 `id-kp-serverAuth`（OID：1.3.6.1.5.5.7.3.1）或 `anyExtendedKeyUsage`（OID：2.5.29.37.0）；及／或，
  - 新憑證的 `basicConstraints` 擴充欄位之 `pathLenConstraint` 為零。

- 若用於 OCSP 回應（例如 BasicOCSPResponse 的 `signatureAlgorithm`）：
  - ResponseData 的 `producedAt` 欄位值**應（MUST）**早於 2022-06-01 00:00:00 UTC；且，
  - 所有未過期、未廢止、包含 CA 金鑰對（Key Pair）之公開金鑰（Public Key），且具有相同主體名稱（Subject Name）之憑證，**應（MUST）**亦包含 `extKeyUsage` 擴充欄位，且其中唯一存在的憑證金鑰用途（key usage）為 `id-kp-ocspSigning`（OID：1.3.6.1.5.5.7.3.9）。

- 若用於 CRL（例如 CertificateList 的 `signatureAlgorithm` 欄位或 TBSCertList 的 `signature` 欄位）：
  - 該 CRL 被一張或多張根憑證機構（Root CA）憑證或下屬憑證機構（Subordinate CA）憑證所參照；且，
  - 該根憑證機構憑證或下屬憑證機構憑證已簽發一張或多張憑證，且已簽發憑證的簽章演算法使用下列 SHA-1 編碼。

**注意**：上述規定不允許 CA 使用下列 SHA-1 編碼簽章預簽憑證。

- 採用 SHA-1 的 RSASSA-PKCS1-v1_5：

  編碼：`300d06092a864886f70d0101050500`

於 2026-09-15 之前，CA **應（SHALL）**廢止所有未過期且憑證中含有 `RSASSA-PKCS1-v1_5 with SHA-1` 之下屬憑證機構（Subordinate CA）憑證。

#### 7.1.3.2.2 ECDSA

CA **應（SHALL）**根據所使用之簽章金鑰選用適當的簽章演算法及編碼。

若簽章金鑰為 P-256，簽章**應（MUST）**使用採用 SHA-256 的 ECDSA。編碼時，`AlgorithmIdentifier` **應（MUST）**與下列十六進位編碼位元組逐位元組完全相同：`300a06082a8648ce3d040302`。

若簽章金鑰為 P-384，簽章**應（MUST）**使用採用 SHA-384 的 ECDSA。編碼時，`AlgorithmIdentifier` **應（MUST）**與下列十六進位編碼位元組逐位元組完全相同：`300a06082a8648ce3d040303`。

若簽章金鑰為 P-521，簽章**應（MUST）**使用採用 SHA-512 的 ECDSA。編碼時，`AlgorithmIdentifier` **應（MUST）**與下列十六進位編碼位元組逐位元組完全相同：`300a06082a8648ce3d040304`。

### 7.1.4 名稱形式（Name Forms）

本節詳述適用於 CA 所簽發之所有憑證的編碼規則。第 7.1.2 節可另行規定進一步限制，但該等限制不得取代本節要求。

#### 7.1.4.1 名稱編碼（Name Encoding）

下列規定適用於第 7.1.2 節所列之所有憑證。具體而言，包括第 7.1.2.3 節所定義之「受技術約束之非 TLS 下屬憑證機構憑證（Technically Constrained Non-TLS Subordinate CA Certificates）」，但不包括由此類 CA 憑證所簽發之憑證，因該等憑證不屬於本《基本要求》之適用範圍。

針對每一條有效的憑證路徑（Certification Path，定義見 RFC 5280 第 6 節）：

- 對於憑證路徑中之每張憑證，其簽發者唯一識別名稱（Issuer Distinguished Name）欄位的編碼內容，**應（SHALL）**與簽發憑證機構（Issuing CA）憑證的主體唯一識別名稱（Subject Distinguished Name）欄位之編碼形式逐位元組完全相同。
- 對於憑證路徑中之每張 CA 憑證，其主體唯一識別名稱（Subject Distinguished Name）欄位的編碼內容，**應（SHALL）**在所有依 RFC 5280 第 7.1 節 比對為相等之主體唯一識別名稱（Subject Distinguished Name）的憑證中逐位元組完全相同（包括已過期及已廢止之憑證）。

編碼 `Name` 時，CA **應（SHALL）**確保：

- 每個 `Name` **應（MUST）**包含一個 `RDNSequence`。
- 每個 `RelativeDistinguishedName` **應（MUST）**包含僅有一個 `AttributeTypeAndValue`。
- 每個 `RelativeDistinguishedName`（若存在）在 `RDNSequence` 中的排列順序，與其於第 7.1.4.2 節之出現順序一致。
  - 例如，包含成對之 `countryName AttributeTypeAndValue` 的 `RelativeDistinguishedName`，**應（MUST）**在 `RDNSequence` 中排列於包含 `stateOrProvinceName AttributeTypeAndValue` 的 `RelativeDistinguishedName` 之前。
- 每個 `Name` 中，任一特定之 `AttributeTypeAndValue` **不得（MUST NOT）**在所有 `RelativeDistinguishedName` 中出現超過一次，除非本文件明確允許。

**注意**：第 7.1.2.2.2 節針對簽發交互認證之下屬憑證機構憑證（Cross-Certified Subordinate CA Certificate），訂有上述 `Name` 編碼要求之例外規定，詳如該節所述。

### 7.1.4.2 主體屬性編碼（Subject Attribute Encoding）

本文件針對 `tbsCertificate` 的 `subject` 欄位中可能出現的若干屬性，定義其內容及驗證要求。除非該等屬性的內容已依第 7.1.2 節指定之相關憑證剖繪（profile）規定完成驗證，且該等屬性為該憑證剖繪所允許，否則 CA **不得（SHALL NOT）**包含該等屬性。

若 CA 在憑證 `subject` 欄位中包含下表所列屬性，**應（SHALL）**依該等屬性於表中出現的相對順序進行編碼，並遵從各屬性的指定編碼要求。

| 屬性 | OID | 規範 | 編碼要求 | 最大長度* |
|---|---|---|---|---|
| `domainComponent` | 0.9.2342.19200300.100.1.25 | RFC 4519 | **應（MUST）**使用 `IA5String` | 63 |
| `countryName` | 2.5.4.6 | RFC 5280 | **應（MUST）**使用 `PrintableString` | 2 |
| `stateOrProvinceName` | 2.5.4.8 | RFC 5280 | **應（MUST）**使用 `UTF8String` 或 `PrintableString` | 128 |
| `localityName` | 2.5.4.7 | RFC 5280 | **應（MUST）**使用 `UTF8String` 或 `PrintableString` | 128 |
| `postalCode` | 2.5.4.17 | X.520 | **應（MUST）**使用 `UTF8String` 或 `PrintableString` | 40 |
| `streetAddress` | 2.5.4.9 | X.520 | **應（MUST）**使用 `UTF8String` 或 `PrintableString` | 128 |
| `organizationName` | 2.5.4.10 | RFC 5280 | **應（MUST）**使用 `UTF8String` 或 `PrintableString` | 64 |
| `surname` | 2.5.4.4 | RFC 5280 | **應（MUST）**使用 `UTF8String` 或 `PrintableString` | 64 [5] |
| `givenName` | 2.5.4.42 | RFC 5280 | **應（MUST）**使用 `UTF8String` 或 `PrintableString` | 64 [5] |
| `organizationalUnitName` | 2.5.4.11 | RFC 5280 | **應（MUST）**使用 `UTF8String` 或 `PrintableString` | 64 |
| `commonName` | 2.5.4.3 | RFC 5280 | **應（MUST）**使用 `UTF8String` 或 `PrintableString` | 64 |

選定屬性的編碼及順序要求

* **注意**：DirectoryString 的 ASN.1 長度限制是以字元數計，而非位元組數。

若 CA 在憑證 `subject` 欄位中包含下表所列屬性，**應（SHALL）**遵從各屬性的指定編碼要求。

| 屬性 | OID | 規範 | 編碼要求 | 最大長度* |
| --- | --- | --- | --- | --- |
| `businessCategory` | 2.5.4.15 | X.520 | **應（MUST）**使用 `UTF8String` 或 `PrintableString` | 128 |
| `jurisdictionCountry` | 1.3.6.1.4.1.311.60.2.1.3 | 《延伸驗證型憑證之簽發與管理指引》（Guidelines for the Issuance and Management of Extended Validation Certificates） | **應（MUST）**使用 `PrintableString` | 2 |
| `jurisdictionStateOrProvince` | 1.3.6.1.4.1.311.60.2.1.2 | 《延伸驗證型憑證之簽發與管理指引》（Guidelines for the Issuance and Management of Extended Validation Certificates） | **應（MUST）**使用 `UTF8String` 或 `PrintableString` | 128 |
| `jurisdictionLocality` | 1.3.6.1.4.1.311.60.2.1.1 | 《延伸驗證型憑證之簽發與管理指引》（Guidelines for the Issuance and Management of Extended Validation Certificates） | **應（MUST）**使用 `UTF8String` 或 `PrintableString` | 128 |
| `serialNumber` | 2.5.4.5 | RFC 5280 | **應（MUST）**使用 `PrintableString` | 64 |
| `organizationIdentifier` | 2.5.4.97 | X.520 | **應（MUST）**使用 `UTF8String` 或 `PrintableString` | 無限制 |

選定屬性的編碼要求

* **注意**：DirectoryString 的 ASN.1 長度限制是以字元數計，而非位元組數。

#### 7.1.4.3 用戶憑證（Subscriber Certificate）之通用名稱（Common Name）屬性

若此屬性存在，**應（MUST）**包含僅有一個項目，且該項目為憑證 `subjectAltName` 擴充欄位中所含值之一（參見第 7.1.2.7.12 節）。該欄位值**應（MUST）**依下列方式編碼：

- 若值為 IPv4 位址，則該值**應（MUST）**依 RFC 3986 第 3.2.2 節 之規定，以 IPv4Address 格式編碼。
- 若值為 IPv6 位址，則該值**應（MUST）**依 RFC 5952 第 4 節 所規定之文字表示方式編碼。
- 若值為完全吻合網域名稱（FQDN）或萬用網域名稱（Wildcard Domain Name），則該值**應（MUST）**逐字元複製 `subjectAltName` 擴充欄位中 `dNSName` 項目的值。具體而言，完全吻合網域名稱的所有網域標籤（Domain Labels），或萬用網域名稱 FQDN 部分的所有網域標籤，均須以 LDH 標籤（LDH Labels）格式編碼，且 P-Labels **不得（MUST NOT）**轉換為 Unicode 表示形式。

#### 7.1.4.4 其他主體屬性

若第 7.1.2 節指定之相關憑證剖繪明確允許，CA **得（MAY）**在 `AttributeTypeAndValue` 中包含第 7.1.4.2 節所述以外的其他屬性。

在包含此類屬性前，CA **應（SHALL）**：

- 在其憑證政策（CP）或憑證實務作業基準（CPS）的第 7.1.4 節中記載該等屬性及適用之驗證作業。
- 確保相關內容所包含的資訊是 CA 於申請者（Applicant）之外，以獨立的方式完成驗證。

### 7.1.5 名稱限制（Name constraints）

參見第 7.1.2.5.2 節「受技術約束之 TLS 下屬憑證機構之名稱限制」及第 7.1.2.10.8 節「憑證機構憑證之名稱限制」。

### 7.1.6 憑證政策物件識別碼（Certificate policy object identifier）

#### 7.1.6.1 保留憑證政策識別碼（Reserved Certificate Policy Identifiers）

下列憑證政策識別碼（Certificate Policy identifiers）保留供 CA 使用，作為宣告憑證遵循本文件要求規定之一種選用方式。

```
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) individual-validated(3)} (2.23.140.1.2.3)

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

### 7.1.7 政策限制（Policy Constraints）擴充欄位之使用

### 7.1.8 政策限定元（Policy qualifiers）之語法與語意

### 7.1.9 關鍵憑證政策（critical Certificate Policies）擴充欄位之語意處理

## 7.2 憑證廢止清冊（CRL）剖繪

於 2024-03-15 之前，憑證機構（Certification Authority，CA）**應（SHALL）**依本文件指定之剖繪，或依《公開信賴憑證簽發與管理之基本要求》（Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates）第 1.8.7 版指定之剖繪簽發憑證廢止清冊（Certificate Revocation List，CRL）。自 2024-03-15 起，CA **應（SHALL）**依本文件指定之剖繪簽發 CRL。

若 CA 聲明其遵循本《基本要求》規定，則其所簽發之所有 CRL **應（MUST）**遵循下列 CRL 剖繪；該剖繪引用 RFC 5280 之相關規定，並以其為基礎衍生。除非另有明確說明，除本文件所規定之規範性要求外，RFC 5280 所定之所有規範性要求亦適用。CA **宜（SHOULD）**參閱 RFC 5280 附錄 B，以瞭解其他應注意事項。

「完整 CRL（full and complete CRL）」係指其涵蓋範圍包含 CA 所簽發之所有憑證的 CRL。

「分割式 CRL（partitioned CRL，有時稱為「分片式 CRL（sharded CRL）」）」係指涵蓋範圍有限的 CRL，例如僅涵蓋 CA 於特定期間所簽發之所有憑證（「時間分片（temporal sharding）」）。除分割式 CRL 含有簽發發布點（Issuing Distribution Point）擴充欄位（OID 2.5.29.28）外，從本剖繪的角度而言，兩種 CRL 格式在語法上相同。

CA **應（MUST）**至少於首次簽發憑證後 7 日內，簽發一份「完整 CRL」，或簽發一組範圍涵蓋該 CA 所簽發之全部憑證的「分割式 CRL」。換言之，若僅簽發分割式 CRL，該等分割 CRL 的合計涵蓋範圍須等同於一份完整 CRL 的涵蓋範圍。

CA **不得（MUST NOT）**簽發間接 CRL（indirect CRL）（即 CRL 簽發者並非該 CRL 涵蓋範圍內的所有憑證簽發者）。

| 欄位 | 必要性 | 說明 |
| --- | --- | --- |
| `tbsCertList` | | |
| `version` | 應（MUST） | 應（MUST）為 v2(1)，參見第 7.2.1 節。 |
| `signature` | 應（MUST） | 參見第 7.1.3.2 節 |
| `issuer` | 應（MUST） | 應（MUST）與簽發憑證機構（Issuing CA）的 `subject` 欄位逐位元組完全相同 |
| `thisUpdate` | 應（MUST） | 表示 CRL 的簽發日期 |
| `nextUpdate` | 應（MUST） | 表示下一份 CRL 的最晚簽發日期。對於範圍涵蓋用戶憑證的 CRL，該日期最遲為 `thisUpdate` 後 10 日；對於其他 CRL，最遲為 `thisUpdate` 後 12 個月。 |
| `revokedCertificates` | * | 若 CA 已簽發之憑證其後遭廢止，且其對應 CRL 條目尚未出現在該廢止憑證有效期屆滿後，至少一份依正常排程簽發的 CRL 中，則 `revokedCertificates` **應（MUST）**存在。當某 CRL 條目已出現在其所對應之遭廢止憑證有效期屆滿後，至少一份依正常排程簽發的 CRL 中，則 CA **宜（SHOULD）**移除該 CRL 條目。其他要求詳見「revokedCertificates 元件」表格 |
| `extensions` | 應（MUST） | 其他要求詳見「CRL 擴充欄位」表格 |
| `signatureAlgorithm` | 應（MUST） | 編碼後之值**應（MUST）**與 `tbsCertList.signature` 逐位元組完全相同 |
| `signature` | 應（MUST） | - |
| 其他任何值 | 不建議（NOT RECOMMENDED） | - |

CRL 欄位

### 7.2.1 版本號

憑證廢止清冊（Certificate Revocation List，CRL）**應（MUST）**為 X.509 v2 版本。

### 7.2.2 憑證廢止清冊（CRL）及 CRL 條目之擴充欄位

| 擴充欄位 | 必要性 | 關鍵性 | 說明 |
| --- | --- | --- | --- |
| `authorityKeyIdentifier` | 應（MUST） | N | 參見第 7.1.2.11.1 節。 |
| `CRLNumber` | 應（MUST） | N | **應（MUST）**包含一個大於或等於 0 且小於 $2^{159}$ 之整數（INTEGER），且該整數與其他 `CRLNumber` 形成嚴格遞增序列。 |
| `IssuingDistributionPoint` | * | Y | 參見第 7.2.2.1 節 憑證廢止清冊（CRL）簽發發布點 |
| 其他任何擴充欄位 | 不建議（NOT RECOMMENDED） | - | - |

CRL 擴充欄位

| 元件 | 必要性 | 說明 |
| --- | --- | --- |
| `serialNumber` | 應（MUST） | **應（MUST）**與已廢止憑證的 `serialNumber` 逐位元組完全相同 |
| `revocationDate` | 應（MUST） | 通常為執行廢止作業的日期及時間。允許倒填日期（backdating）之情形，詳見本表下方注意內容。 |
| `crlEntryExtensions` | * | 其他要求詳見「crlEntryExtensions 元件」表格 |

revokedCertificates 元件

**注意**：若確定憑證的私密金鑰（Private Key）在該憑證的 CRL 條目所載之廢止日期前即已遭破解（compromise），CA **宜（SHOULD）**更新該 CRL 條目中的廢止日期。倒填 `revocationDate` 欄位屬於 RFC 5280 第 5.3.2 節 所述最佳實務之例外；然而，本節要求指定使用 `revocationDate` 欄位，以支援將該欄位所載日期視為憑證首次被認定已遭破解之日期的 TLS 實作。

| CRL 條目擴充欄位 | 必要性 | 說明 |
| --- | --- | --- |
| `reasonCode` | * | 若存在（OID 2.5.29.21），**不得（MUST NOT）**標記為關鍵（critical），且**應（MUST）**指出廢止該憑證之最適當原因。<br><br>除非該 CRL 條目對應之憑證在技術上不具備執行憑證簽發的能力，且符合下列情形之一，否則 `reasonCode` **應（MUST）**存在：(1) 該 CRL 條目對應的是受《基本要求》規範，且於 2023-07-15 之前遭廢止的用戶憑證；或 (2) 廢止原因（即 `reasonCode`）為 unspecified (0)。<br><br>其他要求詳見「CRLReasons」表格。 |
| 其他任何值 | 不建議（NOT RECOMMENDED） | - |

crlEntryExtensions 元件

| RFC 5280 reasonCode | RFC 5280 reasonCode 值 | 說明 |
| --- | --- | --- |
| unspecified | 0 | 以省略 reasonCode 表示。若 CRL 條目對應之憑證在技術上不具備執行憑證簽發的能力，則**應（MUST）**省略 reasonCode，除非該 CRL 條目對應的是受《基本要求》規範，且於 2023-07-15 之前遭廢止的用戶憑證。 |
| keyCompromise | 1 | 表示已知或疑似用戶的私密金鑰已遭破解（compromised）。 |
| affiliationChanged | 3 | 表示憑證中的主體名稱（Subject’ s name）或其他主體識別資訊（Subject Identity Information）已變更，但無理由懷疑該憑證的私密金鑰已遭破解。 |
| superseded | 4 | 表示憑證因下列原因而被取代：用戶已申請新憑證；CA 有合理證據認為，憑證中任一完全吻合網域名稱（FQDN）或 IP 位址的網域授權或控管權驗證不應再受信賴；或 CA 基於符合規範原因而廢止該憑證，例如憑證不遵循本《基本要求》或 CA 的憑證政策（CP）或憑證實務作業基準（CPS）之規定。 |
| cessationOfOperation | 5 | 表示使用該憑證的網站於憑證有效期屆滿前停止運作，或用戶於憑證有效期屆滿前不再擁有或控管該憑證中的網域名稱（Domain Name）。 |
| certificateHold | 6 | 若 CRL 條目所對應的是下列任一憑證，則**不得（MUST NOT）**包含 `certificateHold`：(1) 受《基本要求》規範之憑證；或 (2) 不受《基本要求》規範，且符合下列任一情形之憑證：(A) 於 2020-09-30 當日或之後簽發；或 (B) 其 `notBefore` 為 2020-09-30 當日或之後。 |
| privilegeWithdrawn | 9 | 表示用戶方發生違規情形，但未導致金鑰遭破解（`keyCompromise`），例如憑證用戶在憑證申請（Certificate Request）中提供誤導性資訊，或未履行用戶協議（Subscriber Agreement）或使用條款（Terms of Use）所定之重大義務。 |

CRLReasons

用戶協議（Subscriber Agreement）或其中所參照的線上資源，**應（MUST）**告知用戶上述的廢止原因選項，並說明各選項應於何種情形下選用。CA 提供給用戶的工具，**應（MUST）**允許用戶於請求廢止其憑證時，能輕易指定上述的選項；其預設值應為不提供廢止原因（即預設值對應於 CRLReason「unspecified (0)」，因此 CRL 中不提供 reasonCode 擴充欄位）。

`privilegeWithdrawn` reasonCode **不宜（SHOULD NOT）**作為供用戶選擇的廢止原因選項，因為是否使用此 reasonCode 是由 CA 決定，而非由用戶決定。

若 CA 取得某憑證金鑰遭破解（Key Compromise）的可查證證據，而該憑證的 CRL 條目不含 reasonCode 擴充欄位，或其 reasonCode 擴充欄位所載原因並非 `keyCompromise`，則 CA **宜（SHOULD）**更新該 CRL 條目，將 reasonCode 擴充欄位中的 CRLReason 設為 `keyCompromise`。

#### 7.2.2.1 憑證廢止清冊簽發發布點（CRL Issuing Distribution Point）

分割式 CRL **應（MUST）**包含簽發發布點（Issuing Distribution Point）擴充欄位。簽發發布點擴充欄位中的 `distributionPoint` 欄位**應（MUST）**存在。此外，`DistributionPointName` 欄位值中的 `fullName` 欄位**應（MUST）**存在，且其值**應（MUST）**符合下列要求：

1. 若 CRL 涵蓋範圍內的憑證包含 CRL 發布點（CRL Distribution Points）擴充欄位，則該擴充欄位之 `fullName` 欄位中的 `uniformResourceIdentifier`，至少有一個**應（MUST）**出現在 CRL 簽發發布點（Issuing Distribution Point）擴充欄位的 `fullName` 中。簽發發布點擴充欄位中的 `uniformResourceIdentifier` 值編碼**應（SHALL）**與該憑證 CRL 發布點擴充欄位所使用的編碼逐位元組完全相同。
2. 其他 `uniformResourceIdentifier` 型別的 GeneralName **得（MAY）**包含。
3. 非 `uniformResourceIdentifier` 型別的 GeneralName **不得（MUST NOT）**包含。

`indirectCRL` 及 `onlyContainsAttributeCerts` 欄位**應（MUST）**設為 FALSE（即不設定）。

CA **得（MAY）**依 CRL 的涵蓋範圍，將 `onlyContainsUserCerts` 或 `onlyContainsCACerts` 欄位其中之一設為 TRUE。

CA **不得（MUST NOT）**同時將 `onlyContainsUserCerts` 及 `onlyContainsCACerts` 兩個欄位設定為 TRUE。

`onlySomeReasons` 欄位**不宜（SHOULD NOT）**包含；若包含，CA **應（MUST）**另行提供一份其涵蓋範圍包括所有廢止憑證、不論其 reason code 為何的 CRL。

對於完整 CRL，**不建議（NOT RECOMMENDED）**使用此擴充欄位。

## 7.3 線上憑證狀態協定（OCSP）剖繪

若線上憑證狀態協定（Online Certificate Status Protocol，OCSP）回應是針對根憑證機構（Root CA）憑證或下屬憑證機構（Subordinate CA）憑證（包括交互認證之下屬憑證機構憑證），且該憑證已遭廢止，則 `CertStatus` 之 `RevokedInfo` 中的 `revocationReason` 欄位**應（MUST）**存在。

所指定的 `CRLReason` **應（MUST）**包含第 7.2.2 節規定可用於 CRL 的值。

### 7.3.1 版本號

### 7.3.2 線上憑證狀態協定（OCSP）之擴充欄位

OCSP 回應格式中的 `singleExtensions` **不得（MUST NOT）**包含 CRL 條目擴充欄位所使用的 `reasonCode`（OID 2.5.29.21）。

---

# 8 稽核與其他評估

憑證機構（Certification Authority，CA）在任何時刻均**應（SHALL）**：

1. 遵循《基本要求》規定；
2. 遵循本節所定之稽核要求規定；及
3. 若 CA 營運所在地法律規定，簽發憑證須取得主管機關許可，則 CA 應於各營運所在地取得許可。

## 8.1 稽核頻率或評估事項

具備簽發新憑證能力之憑證，**應（MUST）**符合下列兩者之一：依第 7.1.2.3 節、第 7.1.2.4 節或第 7.1.2.5 節之規定受技術約束，且僅依第 8.7 節之規定接受稽核；或未受技術約束，並依本節其餘所有要求接受完整稽核。憑證若包含 X.509v3 `basicConstraints` 擴充欄位，且 `cA` 布林值設為 TRUE，則視為具備簽發新憑證之能力，因此依定義屬於根憑證機構（Root CA）憑證或下屬憑證機構（Subordinate CA）憑證。

憑證機構（Certification Authority，CA）簽發憑證之期間，**應（SHALL）**劃分為連續且不中斷的稽核期間（Audit Period）。每一個稽核期間**不得（MUST NOT）**超過一年。

若 CA 持有現行有效的稽核報告（Audit Report），且該報告表明其遵循第 8.4 節所列之稽核架構（audit scheme），則無需進行簽發前的整備程度評估。

## 8.2 稽核者之身分與資格

憑證機構（Certification Authority，CA）之稽核**應（SHALL）**由合格稽核業者（Qualified Auditor）執行。合格稽核業者係指自然人（natural person）、法人（Legal Entity），或者由自然人或法人所組成之團體，且其全體具備下列資格與能力：

1. 與稽核對象保持獨立關係；
2. 具備執行稽核之能力，且該稽核涵蓋合格稽核架構所定之準則（參見第 8.4 節）；
3. 雇用具備公開金鑰基礎建設（Public Key Infrastructure，PKI）技術、資訊安全工具及其技術、資訊技術與安全稽核，以及第三方驗證職能等專業能力之人員；
4. （依任一 ETSI 標準進行稽核時）依 ISO 17065 取得認可，並適用 ETSI EN 319 403 所定之要求；
5. （依 WebTrust 標準進行稽核時）取得 WebTrust 授權；

6. 受法律、政府法規或專業倫理守則之約束；及
7. 除政府內部稽核機關（Internal Government Auditing Agency）外，稽核業者應維持專業責任保險（Professional Liability/Errors & Omissions insurance）之投保，其保險金額上限至少為一百萬美元。

## 8.3 稽核者與被稽核實體之關係

## 8.4 稽核涵蓋事項

憑證機構（Certification Authority，CA）**應（SHALL）**依下列稽核架構之一接受稽核：

1. WebTrust：
   - 「憑證機構原則與準則（Principles and Criteria for Certification Authorities）」第 2.2 版或更新版本；以及下列之一：
     - 「WebTrust 憑證機構原則與準則——SSL 基本要求及網路安全（WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security）」第 2.7 版或更新版本；或
     - 「WebTrust 憑證機構原則與準則——SSL 基本要求（WebTrust Principles and Criteria for Certification Authorities – SSL Baseline）」第 2.8 版或更新版本，以及「WebTrust 憑證機構原則與準則——網路安全（WebTrust Principles and Criteria for Certification Authorities – Network Security）」第 1.0 版或更新版本。
2. ETSI：
   - ETSI EN 319 411-1 v1.4.1 或更新版本，其中包含對 ETSI EN 319 401 之規範性引用（所引用之 ETSI 文件應採用最新版本）；或
3. 其他：
   - 若政府憑證機構（Government CA）依其憑證政策（CP）之規定須採用不同的內部稽核架構，則**得（MAY）**採用該內部稽核架構，但其稽核應符合下列任一條件：
     a. 包含上述任一稽核架構之所有要求；或
     b. 由可供公開審查之類似準則所組成。

無論選擇何種稽核架構，該稽核架構**應（MUST）**納入定期監督及／或課責程序，以確保依該稽核架構所進行之稽核，持續遵循該稽核架構之要求。

稽核**應（MUST）**由第 8.2 節所定之合格稽核業者（Qualified Auditor）執行。

對於非企業註冊中心（Enterprise RA）之受委任第三方（Delegated Third Party），CA **應（SHALL）**取得依第 8.4 節所列之認可稽核架構依據的稽核標準所出具的稽核報告；該報告應就受委任第三方之作業執行情形是否遵循其作業基準（practice statement），或是否遵循 CA 的憑證政策（CP）及／或憑證實務作業基

準（CPS）表示意見。若稽核意見認定受委任第三方不遵循前述文件之規定，CA **應（SHALL）**禁止該受委任第三方繼續執行受委託作業（delegated functions）。

受委任第三方之稽核期間**不得（SHALL NOT）**超過一年（理想情況下宜與 CA 之稽核期間一致）。

## 8.5 稽核缺失結果之因應方式

## 8.6 稽核結果之公開

稽核報告（Audit Report）**應（SHALL）**明確載明，其涵蓋所有宣告第 7.1.6.1 節所列一個或多個政策識別碼之憑證簽發所使用的相關系統及流程。憑證機構（Certification Authority，CA）**應（SHALL）**公開稽核報告。

CA **應（MUST）**於稽核期間結束後 3 個月內公開其稽核報告。CA 若延遲超過 3 個月，**應（SHALL）**提供由合格稽核業者（Qualified Auditor）簽署之說明函。

稽核報告**應（MUST）**至少包含下列清楚標示之資訊：

1. 被稽核組織之名稱；
2. 執行稽核之組織名稱及地址；
3. 稽核範圍內所有根憑證機構（Root CA）憑證及下屬憑證機構（Subordinate CA）憑證（包括交互認證之下屬憑證機構憑證）的 SHA-256 指紋；
4. 用於稽核各憑證（及其相關金鑰）之稽核準則及其版本號；
5. 稽核期間所引用之 CA 政策文件清單及其版本號；
6. 稽核之評估期間類型為一段期間或特定時間點；
7. 稽核涵蓋一段期間者，其稽核期間（Audit Period）之起訖日期；
8. 稽核針對特定時間點者，該時間點之日期；
9. 報告出具日期（該日期必然晚於稽核期間之結束日期或該時間點之日期）；及
10. （依任一 ETSI 標準進行稽核時）說明本次稽核為完整稽核或監督稽核，以及所適用及評估的準則內容，例如 DVCP、OVCP、NCP、NCP+、LCP、EVCP、EVCP+、QCP-w、第一部分（一般要求規定）及／或第二部分（信賴服務提供者要求規定）。
11. （依任一 ETSI 標準進行稽核時）說明稽核者已引用適用之 CA/Browser Forum 準則（例如本文件），並載明所引用之版本。

公開稽核資訊**應（MUST）**由合格稽核業者（Qualified Auditor）提供具權威性之英文版本，且 CA **應（SHALL）**確保該版本可公開取得。

稽核報告**應（MUST）**以 PDF 格式提供，且其中所有必要資訊**應（SHALL）**均可用文字進行搜尋。稽核報告中的每一個 SHA-256 指紋**應（MUST）**使用大寫字母，且**不得（MUST NOT）**包含冒號、空格或換行字元。

## 8.7 內部稽核（Self-Audit）

於憑證機構（Certification Authority，CA）簽發憑證期間，CA **應（SHALL）**監督其憑證政策（CP）、憑證實務作業基準（CPS）及本文件要求規定之遵循情形，並至少每季自前次內部稽核樣本抽取範圍之後立即起算之期間內所簽發之憑證中，隨機抽取一張憑證或至少 3% 數量之憑證（以數量較多者為準）作為樣本進行一次內部稽核（Self-Audit），以嚴格管控其服務品質。

自 2025-03-15 起，CA **宜（SHOULD）**採用 Linting 流程，對選定之樣本集中的憑證進行技術準確度驗證，並與先前對同一張憑證所進行之 Linting 作業相互獨立。

除每年接受符合第 8.4 節所定準則之稽核的受委任第三方外，CA **應（SHALL）**由其所僱用之驗證專員（Validation Specialist），持續按季自前次樣本抽取範圍之後的受委任第三方所驗證之憑證中，隨機抽取至少一張憑證或 3% 數量之憑證（以數量較多者為準）作為樣本進行稽核，以嚴格管控由受委任第三方簽發，或含有經受委任第三方驗證之資訊的憑證之服務品質。CA **應（SHALL）**審查每一個受委任第三方之實務作業及程序，以確保該受委任第三方遵循本文件要求規定及相關憑證政策（CP）及／或憑證實務作業基準（CPS）。

CA **應（SHALL）**每年對每一個受委任第三方遵循本文件要求規定之情形進行內部稽核。

於受技術約束之下屬憑證機構（Technically Constrained Subordinate CA）簽發憑證期間，簽章該下屬憑證機構憑證之 CA **應（SHALL）**監督該 CA 之憑證政策（CP）及該下屬憑證機構之憑證實務作業基準（CPS）的遵循情形。該 CA 應至少每季自前次稽核樣本抽取範圍之後立即起算之期間內該下屬憑證機構所簽發之憑證中，隨機抽取一張憑證或至少 3% 數量之憑證（以數量較多者為準）作為樣本，以確保所有適用之憑證政策（CP）均獲遵循。

---

# 9 其他業務與法律事項

## 9.1 費用

### 9.1.1 憑證簽發或展期費用

### 9.1.2 憑證查詢費用

### 9.1.3 憑證廢止或狀態查詢費用

### 9.1.4 其他服務費用

### 9.1.5 退費政策

## 9.2 財務責任

### 9.2.1 保險範圍

### 9.2.2 其他資產

### 9.2.3 對終端個體之保險或保固

## 9.3 業務資訊之保密

### 9.3.1 機密資訊之範圍

### 9.3.2 非屬機密資訊範圍之資訊

### 9.3.3 保護機密資訊之責任

## 9.4 個人資訊之隱私

### 9.4.1 隱私保護計畫

### 9.4.2 視為隱私之資訊

### 9.4.3 不視為隱私之資訊

### 9.4.4 保護隱私資訊之責任

### 9.4.5 使用隱私資訊之告知與同意

### 9.4.6 應司法或行政程序提供資訊

### 9.4.7 其他資訊提供之情形

## 9.5 智慧財產權

## 9.6 聲明與擔保

### 9.6.1 憑證機構（CA）之聲明與擔保

憑證機構（Certification Authority，CA）藉由簽發憑證，向下列憑證受益人（Certificate Beneficiaries）作出本節所列之憑證擔保：

1. 憑證的用戶協議（Subscriber Agreement）或使用條款（Terms of Use）中為當事方之用戶；
2. 與根憑證機構（Root CA）締結契約，約定將該根憑證機構之根憑證納入其所發行軟體的所有應用軟體供應商（Application Software Supplier）；及
3. 合理信賴有效憑證的所有信賴憑證者（Relying Party）。

CA 向憑證受益人聲明及擔保，在憑證有效期內，CA 於簽發及管理該憑證時，遵循本文件要求規定及其憑證政策（CP）及／或憑證實務作業基準（CPS）。

憑證擔保具體包括（但不限於）下列各項：

1. **使用網域名稱或 IP 位址之權利**：CA 於簽發憑證時：
   i. 建立程序，以驗證申請者（Applicant）對憑證 `subject` 欄位及 `subjectAltName` 擴充欄位所列之網域名稱（Domain Name）及 IP 位址（IP address）具有使用權或控管權（或僅就網域名稱而言，已由具有該網域名稱使用權或控管權之人授予該等權利或控管權）；
   ii. 於簽發憑證時遵從該程序；及
   iii. 於 CA 之憑證政策（CP）及／或憑證實務作業基準（CPS）中準確描述該程序；
2. **憑證簽發之授權**：CA 於簽發憑證時：
   i. 建立程序，以驗證主體（Subject）已授權簽發該憑證，且申請者代表（Applicant Representative）已獲授權代表主體申請該憑證；
   ii. 於簽發憑證時遵從該程序；及
   iii. 於 CA 之憑證政策（CP）及／或憑證實務作業基準（CPS）中準確描述該程序；
3. **資訊正確性**：CA 於簽發憑證時：

   i. 建立程序，以驗證憑證所載全部資訊之正確性；
   ii. 於簽發憑證時遵從該程序；及
   iii. 於 CA 之憑證政策（CP）及／或憑證實務作業基準（CPS）中準確描述該程序；
4. **申請者身分**：若憑證中包含主體識別資訊（Subject Identity Information），CA：
   i. 建立程序，依第 3.2 節及第 7.1.2 節驗證申請者身分；
   ii. 於簽發憑證時遵從該程序；及
   iii. 於 CA 之憑證政策（CP）及／或憑證實務作業基準（CPS）中準確描述該程序；
5. **用戶協議**：若 CA 與用戶非屬關係企業（Affiliate），則用戶與 CA 均為符合本文件要求規定之合法有效及可執行用戶協議的當事方；若 CA 與用戶隸屬同一實體或互為關係企業，則由申請者代表確認使用條款；
6. **狀態**：CA 維護一個每週 7 天、每天 24 小時（24x7）均可公開存取之儲存庫（Repository），提供所有未到期憑證之最新狀態（有效或已廢止）資訊；及
7. **廢止**：CA 將基於本文件所定之任一事由廢止憑證。

根憑證機構（Root CA）**應（SHALL）**對下屬憑證機構（Subordinate CA）之履行及擔保、下屬憑證機構對本文件要求規定之遵循，以及下屬憑證機構依本文件要求規定所負之一切責任及賠償義務負責，如同根憑證機構即為簽發該等憑證的下屬憑證機構。

### 9.6.2 註冊中心（RA）之聲明與擔保

不作規定。

### 9.6.3 用戶之聲明與擔保

憑證機構（Certification Authority，CA）**應（SHALL）**要求申請者於用戶協議（Subscriber Agreement）或使用條款（Terms of Use）中，為了 CA 及憑證受益人之利益作出本節所定之承諾及擔保。

於簽發憑證之前，CA **應（SHALL）**為了 CA 及憑證受益人之利益，取得下列任一項：

1. 申請者對其與 CA 之間的用戶協議之同意；或
2. 申請者對使用條款之確認。

CA **應（SHALL）**建立程序，確保每份用戶協議或使用條款均可依法對申請者執行。無論採何種方式，該協議**應（MUST）**適用於依憑證申請所簽發之憑證。CA **得（MAY）**使用電子協議或「點選同意」（click-through）協議，前提是 CA 須確認此類協議可依法執行。每次憑證申請**得（MAY）**個別使用一份協議，亦**得（MAY）**以單一協議涵蓋未來多次憑證申請及其所產生之憑證，但以 CA 向申請者簽發之每張憑證均明確受該用戶協議或使用條款涵蓋為限。

用戶協議或使用條款**應（MUST）**包含要求申請者本身負擔下列義務並作出下列擔保之條款（或基於申請者之分包商、主機代管服務關係，代表其本人或代理人作出下列義務承諾及擔保）：

1. **資訊正確性**：負有義務並擔保，無論於憑證申請時，或 CA 就其提供的憑證之簽發過程另有要求時，均隨時向 CA 提供正確且完整之資訊；
2. **私密金鑰之保護**：申請者負有義務並擔保其將採取一切合理措施，確保隨時控管、保密並妥善保護其所申請憑證中擬包含的公開金鑰（Public Key）之相對應私密金鑰（Private Key），以及任何相關的啟動資料或裝置（例如密碼或 Token）；
3. **憑證之接受**：用戶負有義務並擔保其將確認及驗證憑證內容之正確性；
4. **憑證之使用**：負有義務並擔保，僅將憑證安裝於可透過憑證所列 `subjectAltName` 存取之伺服器，且僅於遵循所有適用法律與用戶協議或使用條款之情形下使用憑證；
5. **通報及廢止**：負有義務並擔保：
   a. 若與憑證所載之公開金鑰相對應的用戶私密金鑰發生任何實際或疑似遭誤用或遭破解，儘速請求廢止該憑證，並停止使用該憑證及相關私密金鑰；及
   b. 若憑證中任何資訊已經或即將變得不正確或不準確，儘速請求廢止該憑證，並停止使用該憑證；
6. **停止使用憑證**：負有義務並擔保，憑證因金鑰遭破解（Key Compromise）而廢止時，應儘速停止使用該憑證所載之公開金鑰相對應的私密金鑰；
7. **回應**：負有義務在指定期限內，回應 CA 就金鑰遭破解或憑證遭誤用的相關指示；
8. **確認及接受**：確認並接受，若申請者違反用戶協議或使用條款之約定，或 CA 的憑證政策（CP）、憑證實務作業基準（CPS）或本《基本要求》之規定須廢止憑證，CA 有權立即廢止該憑證。

### 9.6.4 信賴憑證者之聲明與擔保

### 9.6.5 其他參與者之聲明及擔保

## 9.7 免責聲明

## 9.8 責任限制

對於委託他方執行之任務，憑證機構（Certification Authority，CA）與任何受委任第三方（Delegated Third Party）**得（MAY）**以契約自行約定彼此間之責任分配，但 CA **應（SHALL）**就所有當事人依本文件要求規定之履行負完全責任，視同該等任務未委託他方執行。

若 CA 於簽發及管理憑證時已遵循本文件要求規定及其憑證政策（CP）及／或憑證實務作業基準（CPS），CA **得（MAY）**針對因使用或信賴該憑證所遭受，且超出 CA 的憑證政策（CP）及／或憑證實務作業基準（CPS）所定範圍之任何損失，對憑證受益人或任何其他第三方主張免責。

若 CA 於簽發或管理憑證時未遵循本文件要求規定及其憑證政策（CP）及／或憑證實務作業基準（CPS），CA **得（MAY）**以其所選擇之任何適當方式，針對因使用或信賴該憑證所遭受之一切請求、損失或損害，不論其所涉訴因或法律理論為何，尋求限制其對用戶及信賴憑證者（Relying Party）所負之責任。

若 CA 選擇限制其未遵循本文件要求規定或其憑證政策（CP）及／或憑證實務作業基準（CPS）簽發或管理憑證之責任，CA **應（SHALL）**將該等責任限制納入其憑證政策（CP）及／或憑證實務作業基準（CPS）。

## 9.9 賠償

儘管憑證機構（Certification Authority，CA）對用戶及信賴憑證者（Relying Party）之責任有所限制，CA 瞭解並確認，與根憑證機構（Root CA）訂有根憑證配發協議之應用軟體供應商（Application Software Supplier），並不承擔 CA 依本文件要求規定所負之任何義務或潛在責任，亦不承擔因憑證之簽發或維護，或信賴憑證者及其他人信賴該等憑證，而可能產生之任何義務或潛在責任。因此，除 CA 為政府機關之情形外，CA **應（SHALL）**就各應用軟體供應商因 CA 所簽發之憑證而遭受之一切請求、損害及損失，不論其所涉訴因或法律理論為何，均應協助該應用軟體供應商進行答辯、予以賠償並使其免受損害。惟應用軟體供應商因 CA 所簽發之憑證而遭受之任何請求、損害或損失，係由該應用軟體供應商的軟體直接造成下列情形，則不適用前述規定：將仍屬有效之憑證顯示為不受信賴；或將下列憑證顯示為受信賴：(1) 已過期之憑證；或 (2) 已廢止之憑證（但僅限於 CA 當時已在線上提供該憑證的廢止狀態，而該應用軟體未檢查狀態或忽略憑證已廢止之狀態指示的情形）。

## 9.10 本文件之有效期與終止

### 9.10.1 有效期

### 9.10.2 終止

### 9.10.3 終止及存續之效力

## 9.11 參與者之個別通知與溝通

## 9.12 修訂

### 9.12.1 修訂程序

### 9.12.2 通知機制與期限

### 9.12.3 物件識別碼（OID）必須更改之情況

## 9.13 爭議解決條款

## 9.14 準據法（Governing law）

## 9.15 所遵循之適用法律

憑證機構（Certification Authority，CA）**應（SHALL）**依其於各營運所在地之業務及簽發憑證所適用之相關法律，簽發憑證並營運其公開金鑰基礎建設（Public Key Infrastructure，PKI）。

## 9.16 雜項條款

### 9.16.1 完整協議

### 9.16.2 轉讓

### 9.16.3 可分割性

若本文件要求規定與憑證機構（Certification Authority，CA）營運或簽發憑證所在地之任何法律、法規或政府命令（以下統稱「法律」）發生衝突，CA **得（MAY）**對任何發生衝突的要求進行必要之最小限度修改，以使該要求規定在其所在地合法有效。此規定僅適用於受該法律規範之營運或憑證簽發。在此情形下，CA **應（SHALL）**立即（且於使用修改後之要求規定簽發憑證之前）在其憑證實務作業基準（CPS）第 9.16.3 節中，詳細載明致使 CA 須依本節修改本文件要求規定之法律，以及 CA 對本文件要求規定所實施之具體修改。

CA **應（MUST）**亦（於使用修改後之要求規定簽發憑證之前）傳送訊息至 questions@cabforum.org，並確認該訊息已張貼於公開郵件列表（Public Mailing List）中，且已於 https://cabforum.org/pipermail/public/ 所提供之公開郵件歸檔區（Public Mail Archives）建立索引（或 CA/Browser Forum 另行指定之其他電子郵件地址與連結），藉此將其憑證實務作業基準（CPS）中新增之相關資訊通知 CA/Browser Forum，以供 CA/Browser Forum 據以考量對《基本要求》進行相對應修訂之可能性。

依本節對 CA 實務作業所允許之任何修改，**應（MUST）**於該法律不再適用時，或《基本要求》經修改而得以同時遵循本文件要求規定及該法律時，停止採行。CA **應（MUST）**於 90 日內適當變更其實務作業、修改其憑證實務作業基準（CPS），並依上述方式通知 CA/Browser Forum。

### 9.16.4 契約履行（律師費與權利拋棄）

### 9.16.5 不可抗力

## 9.17 其他條款

---

# 附錄 A CAA 聯絡屬性標籤

這些方法允許網域名稱（Domain Name）擁有者在 DNS 中發布聯絡資訊，以供網域控管權驗證之用。

## A.1 CAA 方法

### A.1.1 CAA contactemail 屬性標籤

語法：`contactemail <rfc6532emailaddress>`

CAA `contactemail` 屬性接受電子郵件地址作為其參數。整個參數值**應（MUST）**為 RFC 6532 第 3.2 節 所定義的有效電子郵件地址，且不得包含任何額外字元或結構，否則不得使用。

以下為網域名稱持有人使用電子郵件地址指定聯絡屬性之範例。

```
DNSZONE

$ORIGIN example.com .
CAA 0 contactemail "domainowner@example.com"
```

若網域名稱擁有者不希望無法解析 `contactemail` 屬性的憑證機構（CA）對該網域名稱簽發憑證，`contactemail` 屬性**得（MAY）**設為關鍵（critical）。

### A.1.2 CAA contactphone 屬性

語法：`contactphone <rfc3966 Global Number>`

CAA `contactphone` 屬性接受電話號碼作為其參數。整個參數值**應（MUST）**為 RFC 3966 第 5.1.4 節 所定義的有效全球號碼（Global Number），否則不得使用。全球號碼**應（MUST）**以 + 開頭並包含國碼，且**得（MAY）**包含空格作為視覺分隔符號。

以下為網域名稱持有人使用電話號碼指定聯絡屬性之範例。

```
DNSZONE

$ORIGIN example.com .
CAA 0 contactphone "+1 555 123 4567"
```

若網域名稱擁有者不希望無法解析 `contactphone` 屬性的憑證機構（CA）對該網域名稱簽發憑證，`contactphone` 屬性**得（MAY）**設為關鍵（critical）。

## A.2 DNS TXT 方法

### A.2.1 DNS TXT 紀錄電子郵件聯絡人（DNS TXT Record Email Contact）

DNS TXT 紀錄**應（MUST）**置於待驗證網域名稱的「`_validation-contactemail`」子網域上。此 TXT 紀錄的整個 RDATA 值**應（MUST）**為 RFC 6532 第 3.2 節 所定義的有效電子郵件地址，且不得包含任何額外字元或結構，否則不得使用。

### A.2.2 DNS TXT 紀錄電話聯絡人（DNS TXT Record Phone Contact）

DNS TXT 紀錄**應（MUST）**置於待驗證網域名稱的「`_validation-contactphone`」子網域上。此 TXT 紀錄的整個 RDATA 值**應（MUST）**為 RFC 3966 第 5.1.4 節 所定義的有效全球號碼（Global Number），否則不得使用。

---

# 附錄 B 對 Onion 網域名稱簽發憑證

本附錄定義在憑證中包含一個或多個 Onion 網域名稱（Onion Domain Name）時所允許採用的驗證程序。

1. 經授權網域名稱（Authorization Domain Name，ADN）**應（MUST）**包含至少兩個網域標籤（Domain Label），其中最右側的網域標籤為「onion」，且緊鄰該「onion」網域標籤左側的網域標籤應為有效的第 3 版 Onion 位址（Version 3 Onion Address），其定義見 Tor Rendezvous 規範－第 3 版 第 6 節。

2. CA **應（MUST）**使用下列至少一種方法驗證申請者對經授權網域名稱（ADN）的控管權：

    1. **（a）** CA **得（MAY）**使用第 3.2.2.4 節中任何載明「此方法允許簽發 Onion 網域名稱」的方法（指第 3.2.2.4 節表格中 Onion 欄位標示「✓」的方法），驗證申請者對經授權網域名稱（ADN）的控管權，但須做以下調整：

使用上述方法驗證申請者對 Onion 網域名稱的控管權時，CA **應（MUST）**使用 Tor 協定建立與經授權網域名稱（ADN）的連線。CA **不得（MUST NOT）**委託第三方建立該連線，亦**不得（MUST NOT）**依賴第三方所建立的連線，例如使用 Tor2Web。

**注意**：本節不凌駕或取代各驗證方法本身所規定的任何內容。CA **應（MUST）**僅在該方法於其所屬章節中仍獲准使用時使用該方法。

2. **（b）** 若 `certificationRequestInfo` 的 Attributes 區段包含下列內容，CA **得（MAY）**要求申請者提供以 .onion 服務私密金鑰（private key）簽章的憑證請求（Certificate Request），以驗證申請者對經授權網域名稱（ADN）所對應之 .onion 服務的控管權：
   - **（i）** `caSigningNonce` 屬性，其中包含由 CA 產生的隨機值（Random Value）；及
   - **（ii）** `applicantSigningNonce` 屬性，其中包含單一值。CA **應（MUST）**向申請者建議，`applicantSigningNonce` 值宜包含至少 64 位元之亂度（entropy，資訊熵）。

   簽章 nonce（signing nonce）屬性的格式如下：

```ASN.1
cabf OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(14
0) }

caSigningNonce ATTRIBUTE ::= {
   WITH SYNTAX              OCTET STRING
   EQUALITY MATCHING RULE   octetStringMatch
   SINGLE VALUE             TRUE
   ID                       { cabf-caSigningNonce }
}

cabf-caSigningNonce OBJECT IDENTIFIER ::= { cabf 41 }

applicantSigningNonce ATTRIBUTE ::= {
   WITH SYNTAX              OCTET STRING
   EQUALITY MATCHING RULE   octetStringMatch
   SINGLE VALUE             TRUE
   ID                       { cabf-applicantSigningNonce }
}

cabf-applicantSigningNonce OBJECT IDENTIFIER ::= { cabf 42 }
```

   隨機值自建立之日起，用於確認回覆的有效期限**應（SHALL）**不超過 30 日。憑證實務作業基準（Certification Practice Statement，CPS）**得（MAY）**規定更短的隨機值有效期限。

3. 若憑證中包含 Onion 網域名稱，且該憑證係依本文件附錄 B 規定所簽發，則該網域名稱不視為內部名稱（Internal Name）。

**註腳**

1. 有關此擴充欄位之進一步要求，包括是否標記為關鍵（critical）的相關要求，參見。

   回到內文： § 7.1.2.2.3　§ 7.1.2.3.1　§ 7.1.2.4.1　§ 7.1.2.5.1　§ 7.1.2.6.1

2. 雖然 指出，此擴充欄位通常僅出現於終端個體憑證，但本文件利用此擴充欄位以限制 CA 憑證（根憑證除外）的適用範圍；藉由此種限制，可進一步保護信賴憑證者（Relying Party），且此做法已由多家應用軟體供應商實作。

   回到內文： § 7.1.2.2.3 [2]　§ 7.1.2.3.1　§ 7.1.2.4.1　§ 7.1.2.5.1　§ 7.1.2.6.1

3. 雖然 允許 `PolicyInformation` 以任意順序出現，但部分用戶端實作所採用的程式邏輯會考量符合特定篩選條件的 `policyIdentifier`。因此，確保含有保留憑證政策識別碼（Reserved Certificate Policy Identifier）之 `PolicyInformation` 位於首位，可降低發生交互運作問題之風險。

   回到內文： § 7.1.2.2.6　§ 7.1.2.7.9　§ 7.1.2.10.5

4. 若 CA 憑證未設定 `digitalSignature` 旗標位元，CA 私密金鑰**不得（MUST NOT）**用於簽章 OCSP 回應。更多資訊詳見。

   回到內文： § 7.1.2.10.7

5. **注意**：雖然 規定上限為 32,768 個字元，但此係轉錄 X.520（2005 年 8 月版）時所產生之筆誤。有效（可交互運作）的上限為 64 個字元。

   回到內文： § 7.1.4.2 [2]