更新日期：2004-05-14

# 附表二 PKI-Based 應用系統對公鑰憑證處理之安全檢查表
（註：適用於使用舊 GCA 憑證的系統）

| 安全檢查項目 | 是否合格 |
|---|---|
| 系統應該由安全管道取得 GCA 的自簽憑證（Self-Signed Certificate），並妥善地安全保存於系統中。 | □ 是 □ 否 |
| 系統應該檢查用戶的憑證確實為GCA所簽發之憑證（至少需檢查用戶憑證的 Issuer Name (DN)是否與GCA 自簽憑證的 Subject Name(DN)相符，並以 GCA 自簽憑證所記載的 Public Key 檢驗用戶憑證的簽章）。 | □ 是 □ 否 |
| 系統應該檢查用戶的憑證是否仍在有效期限之內（例如檢查系統時間是否仍落在憑證所記載的 Validity 時間範圍內）。<br>注意：憑證是以世界標準時間（UTC，或稱為格林威治時間）來記載 Validity 時間範圍，因此系統不應拿本地時間（Local Time）直接與憑證 Validity 時間範圍相比較。 | □ 是 □ 否 |
| 系統應該檢查用戶的憑證是否已被廢止（例如定期下載 GCA 簽發的 CRL 來檢查憑證廢止狀態）。 | □ 是 □ 否 |
| 系統應該檢查 CRL 是否確實為 GCA 所簽發（至少需檢查 CRL 的 Issuer Name (DN)是否與 GCA 自簽憑證的 Subject Name(DN)相符，並以 GCA 自簽憑證所記載的 Public Key 檢驗 CRL 的簽章）。 | □ 是 □ 否 |
| 系統應該檢查 CRL 是否為最新公佈的 CRL（當天公佈的 CRL）。<br>注意：CRL 的更新時間也是是以世界標準時間（UTC，或稱為格林威治時間）來記載，因此系統不應拿本地時間（Local Time）直接與 CRL 的更新時間相比較。 | □ 是 □ 否 |
| 系統應該要求用戶對傳送的訊息加簽電子簽章以驗證用戶身分。 | □ 是 □ 否 |
| 系統應該要具備防止或偵測用戶加簽之訊息遭到非法重送（Replay）的機制（例如在加簽訊息中加入 Challenge-Response 或 Nonce 機制）。 | □ 是 □ 否 |
| 系統傳送用戶隱私資料時應該要以強度 128 bits 以上的安全通道加以保護（例如使用 SSL 安全通道或是對傳送的訊息以數位信封加密）（若系統並不涉 | □ 是 □ 否 □ 不適用 |

| 安全檢查項目 | 是否合格 |
| --- | --- |
| 及傳送用戶隱私資料時，則本項不適用）。 | |
| 系統應該定期校時，以保持系統時間之正確性(例如定期透過 NTP 自動教時)。 | □ 是 □ 否 |