應用系統使用公鑰憑證處理之安全檢查表

109年9月

說明：為確保各機關(構)開發之應用系統使用政府核發之憑證進行身分認證或數位簽章之安全性，爰訂定下列安全檢查項目，請各機關(構)於驗收時，應確實檢查符合性。

項次	安全檢查項目	檢查結果
1	系統應由安全管道取得 Root CA 的自簽憑證(Self-Signed Certificate)，並妥善安全保存於系統中	☐ 通過 ☐ 不通過
2	系統應設定所信賴的憑證保證等級，並檢查憑證之憑證政策(Certificate Policies)欄位所記載的 Policy OID 是否符合憑證保證等級的要求，對於不符保證等級之憑證應拒絕存取(例如正式上線系統應對測試等級的憑證加以拒絕)	☐ 通過 ☐ 不通過
3	系統應檢查 CA 本身憑證確為 Root CA 所簽發的憑證 (至少需檢查憑證的 Issuer Name (DN)是否與 Root CA 自簽憑證的 Subject Name(DN)相符，並以 Root CA 自簽憑證所記載的 Public Key 檢驗 CA 本身憑證的簽章)	☐ 通過 ☐ 不通過
4	系統應檢查 CA 本身憑證確實為合法的 CA 憑證(Basic Constraints 欄位標示為 CA 憑證)，且憑證之金鑰用途(KeyUsage)欄位允許	☐ 通過 ☐ 不通過

項次	安全檢查項目	檢查結果
	keyCerSign 及 cRLSign 的用途	
5	系統應檢查 CA 本身憑證是否在效期內(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) 注意：憑證是以世界標準時間(UTC，或稱格林威治時間)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	☐ 通過 ☐ 不通過
6	系統應檢查 CA 本身憑證是否已被廢止(例如定期下載 Root CA 簽發的憑證機構廢止清冊(CARL)檢查憑證廢止狀態)	☐ 通過 ☐ 不通過
7	系統應檢查 CARL 是否確實是 Root CA 所簽發(至少需檢查 CARL 的 Issuer Name (DN)是否與 Root CA 自簽憑證的 Subject Name(DN)相符，並以 Root CA 自簽憑證所記載的 Public Key 檢驗 CARL 的簽章)	☐ 通過 ☐ 不通過
8	系統應檢查是否為最新的 CARL(當天公布的 CARL) 注意：CARL 的更新時間是以世界標準時間來記載，因此系統不應拿本地時間直接與 CARL 的更新時間相比較	☐ 通過 ☐ 不通過

項次	安全檢查項目	檢查結果
9	系統應檢查用戶的憑證為合法 CA 所簽發(至少需檢查用戶憑證的 Issuer Name (DN)是否與 CA 憑證的 Subject Name(DN)相符，並以 CA 憑證所記載的 Public Key 檢驗用戶憑證的簽章)	☐ 通過 ☐ 不通過
10	系統應檢查用戶憑證金鑰用途(KeyUsage)欄位所記載的金鑰用途符合使用目的(簽章/驗簽，或加密/解密)	☐ 通過 ☐ 不通過
11	系統應檢查用戶的憑證是否在效期內(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) 注意：憑證是以世界標準時間來記載，因此系統不應拿本地時間直接與憑證 Validity 時間範圍相比較	☐ 通過 ☐ 不通過
12	系統應檢查用戶的憑證是否已被廢止(例如定期下載 CA 簽發的憑證廢止清冊(CRL)檢查憑證廢止狀態，或透過 OCSP 來檢查憑證廢止狀態)	☐ 通過 ☐ 不通過
13	系統應檢查 CRL 是合法 CA 所簽發(至少需檢查 CRL 的 Issuer Name (DN)是否與 CA 本身憑證的 Subject Name(DN)相符，並以 CA	☐ 通過 ☐ 不通過 ☐ 不適用

項次	安全檢查項目	檢查結果
	本身憑證所記載的 Public Key 檢驗 CRL 的簽章)，如果使用 OCSP 查詢，則本項不適用	
14	系統應檢查是否為最新公佈的 CRL(當天公布的 CRL)，如果使用 OCSP 查詢，則本項不適用 注意：CRL 的更新時間是以世界標準時間來記載，因此系統不應拿本地時間直接與 CRL 的更新時間相比較	☐ 通過 ☐ 不通過 ☐ 不適用
15	系統應要求用戶對傳送的訊息加簽電子簽章以驗證用戶身分	☐ 通過 ☐ 不通過
16	系統應具備防止用戶加簽之訊息遭到非法重送(Replay)之功能(例如在加簽訊息中加入 Challenge-Response 或 Nonce 機制)	☐ 通過 ☐ 不通過
17	系統傳送用戶隱私資料時應以強度128 bits 以上的安全通道進行保護(例如使用 SSL 安全通道或是對傳送的訊息以數位信封加密)，若系統未涉及傳送用戶隱私資料時，則本項不適用	☐ 通過 ☐ 不通過 ☐ 不適用
18	系統應定期校時，以保持系統時間之正確性(例如定期透過 NTP 自動校時)	☐ 通過 ☐ 不通過
19	系統應檢查用戶的憑證授權狀態是否符合資	■ 不適用

項次	安全檢查項目	檢查結果
	格，對於未取得授權的憑證應拒絕存取(例如定期下載 OAS(Online Authorization Status)平臺簽發的 CASL(Certificate Authorized Status List)檢查憑證授權狀態，或透過 OASP(Online Authorization Status Protocol)檢查憑證授權狀態)	政府憑證附卡授權機制已停止服務，憑證應用系統無須檢查此項目
20	系統應檢查是否為最新的 CASL(當天公布的 CASL)，如果使用 OASP 查詢，則本項不適用 注意：CASL 的更新時間是以世界標準時間來記載，因此系統不應拿本地時間直接與 CASL 的更新時間相比較	■ 不適用 政府憑證附卡授權機制已停止服務，憑證應用系統無須檢查此項目
21	系統應檢查 CASL 是否確實為 OAS 所簽發(至少需檢查 CASL 的 Issuer Name (DN)是否與 OAS 本身憑證的 Subject Name(DN)相符，並以 OAS 本身憑證所記載的 Public Key 檢驗 CAS 的簽章)，如果使用 OASP 查詢，則本項不適用	■ 不適用 政府憑證附卡授權機制已停止服務，憑證應用系統無須檢查此項目

備註：未來政府若產製下一代新的憑證，應用系統亦應依上列安全檢查項目對下一代新的憑證進行檢查。