應用系統使用公鑰憑證處理安全檢核說明

注意：使用 TWCA 簽發之 SSL 憑證之應用系統包含但不限於 Web Server 及 Web Browser，以下以主流市場之 Web Server(例如：Apache, IIS)及瀏覽器(IE, Chrome, Firefox, Safari)進行檢核說明。

項次	安全性檢查項目	檢核說明	檢查結果
1.	系統應該由安全管道取得 Root CA 的自簽憑證(Self-Signed Certificate)，並妥善地安全保存於系統中。	TWCA 之 Root CA 自簽憑證目前由作業系統或 Web Browser 預先安裝於產品內，且經廠商(例如 Microsoft 或 Apple)以數位簽章加以保護不會被竄改。	通過
2.	系統應該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，並對於不符保證等級的憑證應以拒絕存取(例如正式上線系統應對測試等級的憑證加以拒絕)。	信賴 TWCA 簽發之 SSL 憑證之瀏覽器或作業系統，已預先設定好 CA Browser Forum 針對 SSL 憑證制定的 Policy OID，包含網域驗證(Domain Validation)、組織驗證(Organization Validation)及延伸驗證(Extended Validation)。	通過
3.	系統應該檢查 CA 本身的憑證確實為 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)。	瀏覽器係以 IETF RFC-5280(或更新版本)規定之方式進行憑證檢驗，符合本項要求。	通過
4.	系統應該檢查 CA 本身的憑證確實為合法的 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 keyCertSign 及 cRLSign 的用途。	瀏覽器係以 IETF RFC 5280(或更新版本)規定之方式進行憑證 Basic Constraints 欄位及金鑰用途檢驗，符合本項要求。	通過
5.	系統應該檢查 CA 本身的憑證是否仍在有效期限內(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	瀏覽器係以 IETF RFC 5280(或更新版本)規定之方式進行憑證有效期限之檢驗，符合本項要求。	通過
6.	系統應該檢查 CA 本身的憑證是否已被廢止(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)。	瀏覽器係以 IETF RFC 5280(或更新版本)及 RFC-6960 規定之方式進行 CA 憑證廢止之檢驗，符合本項要求。	通過
7.	系統應該檢查 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	瀏覽器係以 IETF RFC 5280(或更新版本)規定之方式進行 CARL 簽發者之檢驗，符合本項要求。	通過

	載的 Public Key 檢驗 CARL 的簽章)。		
8.	系統應該檢查 CARL 是否為最新的 CARL(當天公佈的 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	瀏覽器係以 IETF RFC 5280(或更新版本)規定之方式進行 CARL 更新時間之檢驗，符合本項要求。	通過
9.	系統應該檢查用戶的憑證確實為合法 CA 所簽發的憑證(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 CA 本身憑證的簽章)。	瀏覽器係以 IETF RFC-5280(或更新版本)規定之方式進行憑證檢驗，符合本項要求。	通過
10.	系統應該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/驗章，或加密/解密)。	瀏覽器係以 IETF RFC 5280(或更新版本)規定之方式進行憑證 Basic Constraints 欄位及金鑰用途檢驗，符合本項要求。	通過
11.	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)。 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。	瀏覽器係以 IETF RFC 5280(或更新版本)規定之方式進行憑證有效期限之檢驗，符合本項要求。	通過
12.	系統應該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)。	瀏覽器係以 IETF RFC 5280(或更新版本)及 RFC-6960 規定之方式進行憑證廢止之檢驗，符合本項要求。	通過
13.	系統應該檢查 CRL 是否確實是合法 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 本身憑證所記載的 Public Key 檢驗 CRL 的簽章)。	瀏覽器係以 IETF RFC 5280(或更新版本)規定之方式進行 CRL 簽發者之檢驗，符合本項要求。	通過
14.	系統應該檢查 CRL 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	瀏覽器係以 IETF RFC 5280(或更新版本)規定之方式進行 CRL 更新時間之檢驗，符合本項要求。	通過
15.	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。	網站伺服器(Web Server)使用 SSL 憑證，在與瀏覽器建立加密通道前，會先遞送電子簽章訊息供瀏覽器以 SSL 憑證驗證網站	通過

		之電子簽章。	
16.	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)之功能(例如在加簽訊息中加入 Chellenge-Response 或 Nouce 機制)。	網站伺服器(Web Server)使用 SSL 憑證，在與瀏覽器建立加密通道前，會在加簽訊息中加入 Chellenge-Response。	通過
17.	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)，若系統未涉及傳送用戶隱私資料時，則本項不適用。	目前網站使用之通訊協定 TLS 1.2，其加密強度至少有 128 bits。	通過
18.	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 自動校時)。	執行瀏覽器之電腦為不特定終端用戶，僅能公告建議用戶定期進行校時。	不適用
19.	系統應檢查用戶的憑證授權狀態是否符合資格，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)平台簽發的 CASL(Certificate Authorization Status Protocol)檢查憑證授權狀態)	SSL 憑證不適用	不適用
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	SSL 憑證不適用	不適用
21.	系統應該檢查 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 CASL 的簽章)，如果使用 OASP 查詢，則本項不適用。	SSL 憑證不適用	不適用