應用系統使用數位身分識別證（New eID）之安全檢查表

內政部109年12月

一、適用於面對面身分識別(非電子查驗)

項次	安全檢查項目	檢查結果
1	核對手上所持New eID當事人人貌及卡面個人資料是否相符	□通過 □不通過
2	檢查New eID卡片防偽機制	□通過 □不通過
3	使用New eID領補換資料查詢作業(https://www.ris.gov.tw)，查詢該New eID是否為有效New eID	□通過 □不通過
4	若需取得當事人隱性資料，須請當事人出示戶口名簿、戶籍謄本或New eID晶片資料清單搭配New eID使用，及依相關文件查驗流程進行驗證	□通過 □不通過

二、適用於面對面身分識別(公開區/加密區電子查驗)

項次	安全檢查項目	檢查結果
1	系統應該由安全管道取得授權管理CA(Country Signing Certificate Authority, CSCA)的自簽憑證（Self-Signed Certificate），並妥善地安全保存於系統中	□通過 □不通過
2	系統應該檢查證件簽署憑證(Document Signer Certificate, DSC)確實為CSCA所簽發的憑證（至少需檢查憑證的 Issuer Name (DN)是否與CSCA自簽憑證的Subject Name(DN)相符，並以CSCA自簽憑證所記載的Public Key檢驗DSC的簽章）	□通過 □不通過
3	系統應該檢查DSC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）	□通過 □不通過
4	系統應該檢查DSC是否已被廢止（例如定期下載CSCA簽發的憑證廢止清冊(Certificate Revocation List, CRL)來檢查憑證廢止狀態）	□通過 □不通過
5	系統應該檢查 CRL是否為最新公佈的 CRL，且該CRL為CSCA所簽發	□通過 □不通過
6	系統應該檢查當事人的New eID邏輯資料結構(Logical Data Structure, LDS)確實為DSC所簽發的（至少需檢查LDS中的簽章者資訊與DSC相符，並以DSC所記載的Public Key檢驗LDS的簽章）	□通過 □不通過
7	系統應該檢查New eID是否已被廢止(例如定期下載New eID廢止清冊或使用線上New eID狀態查詢服務)	□通過 □不通過
8	系統應該檢查New eID廢止清冊是否為最新公佈的廢止清冊，且為內政部所簽發	□通過 □不通過
9	核對LDS中的照片與持有New eID當事人人貌及基本資料是否相符	□通過 □不通過

三、適用於網路身分識別(自然人憑證數位簽章輔以公開區/加密區電子查驗)

項次	安全檢查項目	檢查結果
1	系統應該依據 PKI-Based 應用系統對公鑰憑證處理之安全檢查表檢查自然人憑證數位簽章	□通過 □不通過
2	系統應該由安全管道取得授權管理 CA(Country Signing Certificate Authority, CSCA)的自簽憑證（Self-Signed Certificate），並妥善地安全保存於系統中	□通過 □不通過
3	系統應該檢查證件簽署憑證(Document Signer Certificate, DSC)確實為 CSCA 所簽發的憑證（至少需檢查憑證的 Issuer Name (DN)是否與 CSCA 自簽憑證的 Subject Name(DN)相符，並以 CSCA 自簽憑證所記載的 Public Key 檢驗 DSC 的簽章）	□通過 □不通過
4	系統應該檢查 DSC 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）	□通過 □不通過
5	系統應該檢查 DSC 是否已被廢止（例如定期下載 CSCA 簽發的憑證廢止清冊(Certificate Revocation List, CRL)來檢查憑證廢止狀態）	□通過 □不通過
6	系統應該檢查 CRL 是否為最新公佈的 CRL，且該 CRL 為 CSCA 所簽發	□通過 □不通過
7	系統應該檢查當事人的 New eID 邏輯資料結構(Logical Data Structure, LDS)確實為 DSC 所簽發的（至少需檢查 LDS 中的簽章者資訊與 DSC 相符，並以 DSC 所記載的 Public Key 檢驗 LDS 的簽章）	□通過 □不通過
8	系統應該檢查 New eID 是否已被廢止(例如定期下載 New eID 廢止清冊或使用線上 New eID 狀態查詢服務)	□通過 □不通過
9	系統應該檢查 New eID 廢止清冊是否為最新公佈的廢止清冊，且為內政部所簽發	□通過 □不通過
10	系統應該比對憑證內記載的鏈結資訊與公開區記載的鏈結資訊是否相符	□通過 □不通過

注意：憑證及 CRL 中記載的時間是以世界標準時間（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）直接與憑證/CRL 的時間相比較。