附表一、 數位身分驗證機制與信賴等級對照表

信賴等級	說明	身分登錄	信物管理	身分驗證	實務做法
等級一: 低 (LOA1)	• 對利用特定數位身分驗證機制所驗證客戶宣稱之身分，只有少許信心或幾乎沒有信心； • 於身分驗證失效時產生之風險屬低風險者。	自我聲明或自我宣稱。	無特定要求。	驗證結果僅提供最低程度的身分信任。	無法辨識客戶真實身分，信物核發由客戶自行主張，至少應有客戶帳號與密碼建立基本驗證機制。
等級二: 中 (LOA2)	• 對利用特定數位身分驗證機制所驗證客戶宣稱之身分有中等程度之信心； • 對於身分驗證失效產生之風險屬中風險者。	具有一個機構登錄與核驗客戶資料，並使用安全註冊方式降低竊聽與猜測之風險。	信物需進行管控，且必須具備保護儲存信物的機制。	• 單因子驗證。 • 透過可信賴之機構驗證來源的身分資訊進行驗證。	具有一個機構(不限會員公司本身或是公正第三方)登錄與核驗客戶資料、持有一種信物，以及安全的身分驗證方式，如合併使用不同類型的安全設計，則可提升為信賴等級三之高信賴等級。
等級三: 高 (LOA3)	• 對利用特定數位身分驗證機制所驗證客戶宣稱之身分有高度之信心； • 對於身分驗證失效產生之風險屬高風險者。	基於等級三之身分登錄內容，至少一個(含)以上機構登錄與核驗客戶資料，並使用安全註冊方式降低竊聽與猜測之風險。	• 信物需進行管控，且必須具備保護儲存信物的機制。 • 身分驗證過程在傳輸和儲存時需透過加密保護。	• 多因子驗證。 • 透過可信賴之機構的身分資訊進行驗證，並額外進行身分資訊確認。	至少具有一個機構(不限會員公司本身或是公正第三方)登錄與核驗客戶資料，並採用多因子認證管理機制，且身分認證過程的機敏資料傳輸與儲存均應加密保護。
等級四: 極高 (LOA4)	• 對利用特定數位身分驗證機制所驗證客戶宣稱之身分有非常高之信心；	• 客戶需面對面進行身分登錄，確保身分真實性。	• 所有金鑰需儲存在防篡改硬體中。 • 敏感資料需在傳輸和	• 多因子驗證，且需採用金鑰或數位憑證。 • 透過多個可信賴之機	基於等級三之作業內容，並於身分註冊時應採親晤(面對面)或使用具有

	• 對於身分驗證失效產生之風險屬極高風險者。	• 客戶本人親自與會員公司採面對面方式完成身分登錄。	儲存中全面加密保護。	構的身分資訊進行驗證。 • 進行身分真實性資訊確認。	防偽機制之視訊軟體核驗身分，並使用防篡改硬體設備儲存信物，所有機敏資料傳輸與靜態保存時應採加密保護。