臺灣集中保管結算所股份有限公司 112 年度研究報告提要表		填表人：周儒 填表日期：112 年 12 月 20 日	
研究項目	**集保結算所數位身分驗證現況與應用場景評估**		
研究單位及人員	企劃部：許傳昌、王秀芬、簡易賜、朱月桂、林欣賢、周儒、丁景麟 業務部：王博玄 數位暨資安部：劉家亨、李兆文	研究時間	112 年 1 月至 12 月
報告內容摘要			

壹、研究內容重點

本研究蒐集國際數位身分驗證機制及法規制度，並整理適用臺灣金融業實務及國際主要框架，歸納針對集保結算所現行各應用系統身分驗證現況進行歸納整理，並評估多元數位身分驗證機制可應用之業務場景，設計集保結算所全公司適用的數位身分驗證框架。

國際上對於數位身分之管理以及身分驗證，訂定了不同的管理規章及國際標準，如歐盟 eIDAS、美國 NIST800-63-3 及國際標準化組織制定的 ISO/IEC 29115，針對數位身分驗證相關規範，進一步分析兩者的差異，從中發展適合集保結算所之身分驗證框架。另以數位身分政策與信賴框架為主題，介紹澳洲、瑞典、新加坡及 FIDO 聯盟等國際數位身分的應用發展。

為研擬適用集保結算所的數位身分驗證框，本研究參考 ISO29115 個體身分驗證信賴框架，建立差異化的風險信賴等級且分級制的監督管理機制，並按照數位身分驗證評估流程，彙整集保結算所現有各項內外部系統之用戶類型、角色、交易類型等基本資料，進行身分驗證錯誤對系統的影響評估，以確認所對應之業務信賴等級需求，並依信賴等級評估與挑選身分驗證機制，以及確認所採用之驗證機制，產出應用系統身分驗證評估摘要，日後並依 ISO27001 規範定期檢視。

本研究以手機摺系統為例，參考數位身分驗證評估流程，包括彙整基本資料、風險影響評估、確認對應之 LoA 需求、依 LoA 評估身分識別與驗證機制、確認所採用之身分驗證機制，及產出應用系統身分驗證評估摘要。

貳、結論與建議

本研究經彙整主管機關推動之數位身分驗證機制政策，以及國際數位身分驗證標準與規範，擷取可作為集保結算所建構數位身分驗證框架之參採內容，建議如下：

建議一：集保結算所各業務系統依本研究框架，進行盤點分析及確認推動順序及時程

(一)依集保結算所業務特性，規劃設計數位身分驗證框架，參照身分登錄、信物管理及驗證三個階段，將風險等級與驗證機制分級。

(二)依照數位身分驗證評估流程，彙整各項系統之用戶類型、角色、交易類型等基本資料，進行身分驗證錯誤對系統的影響評估。

建議二：依據數位身分驗證框架，制定集保結算所 ISO 程序文件，作為各業務應用場景應用之參照

(一)集保結算所現行系統，應依照數位身分驗證框架及優先順序，依據風險、成本及相關衝擊性，循序漸進逐步導入。

(二)針對新系統需求開發，應共同討論判斷該系統之身分驗證等級與驗證機制；屬提供自然人客戶之數位服務，須配合金管會「金融服務業辦理數位身分驗證指引」，納入內控制度並定期檢視。

(三)考量集保結算所多項 B2B 系統，參加人指定自然人執行職務，建議研議一致的數位身分驗證規範，提供全公司內外部系統共同遵循。