金融服務業辦理數位身分驗證指引說明對照表

指引內容	說明
一、 為提供民眾便利、快速、安全之數位金融服務，並協助金融服務業運用適當之數位身分驗證機制以降低潛在之風險，特訂定本指引。 本指引所稱金融服務業係指「金融監督管理委員會組織法」第二條第二項之金融服務業。	一、 第一項明定本指引訂定目的，係為就金融服務業辦理數位身分驗證建立一跨業共通性語言及應用原則，以提供民眾便利、快速、安全之數位金融服務。本指引性質為行政指導。 二、 第二項明確揭示本指引所稱金融服務業係指「金融監督管理委員會組織法」第二條第二項之金融服務業。
二、 金融服務業辦理數位身分驗證，除應遵循個人資料保護法、洗錢防制及打擊資恐等相關法令、各金融服務業別之內部控制及稽核制度、電子業務、金融資安控管等相關規定與自律規範，及金融周邊單位相關規章辦理外，並依本指引辦理。 本指引適用於金融服務業辦理自然人之數位身分驗證。	一、 第一項明定金融服務業辦理數位身分驗證除應遵循之相關法令、各金融服務業別（下稱各業別）之相關規定與自律規範及金融周邊單位相關規章外，並依本指引辦理。 二、 各業別依業務特性並非均訂有數位身分驗證之相關規範。考量金融科技變化快速，為促進數位金融服務之發展，提供業者辦理數位身分驗證之彈性，若各業別法規命令、自律規範及規章未訂有數位身分驗證之規範，或其所定規範未含括可能之新式數位金融服務應用場景或新式數位身分驗證方式，各業別可參考本指引訂定相關自律規範或規章

❖建議併同參閱說明欄

	內容，或由業者依本指引辦理；若各業別法規命令、自律規範及規章已訂有數位身分驗證之規範，則各業別可參考本指引之原則，評估調整其自律規範或規章之規範內容。 三、 第二項明確揭示本指引僅適用於金融服務業辦理自然人之數位身分驗證；法人部分於未來研議納入。 四、 數位身分驗證過程中之認識客戶、盡職調查、客戶意思表示或授權及其信物之產製等，應依現行相關規定辦理，非本指引涵蓋範疇。
三、 本指引所稱數位身分驗證(Digital Identity Authentication)，係指在數位金融環境利用適當之技術，確保客戶為其所宣稱身分之過程。 數位身分驗證機制包含「身分登錄(identity enrollment)」、「信物管理(credential management)」及「身分驗證(identity authentication)」三階段。客戶於首次啟用數位金融服務時，金融服務業透過「身分登錄」及「信物管理」作業，以核驗並確認客戶所提供之身分資料與客戶本身之關聯性，並綁定、核發及啟用信物。嗣後客戶於每次使用數位金融服務時，金融服務業透過「身分驗證」作業，依據客戶所提示信物及身分驗證協定確認客戶身分(詳參附圖一)。 數位身分驗證機制之參與者如下：	一、 第一項參考 ISO/IEC 29115 就數位身分驗證予以定義。 二、 參考 ISO/IEC 29115，數位身分驗證機制包含身分登錄、信物管理及身分驗證等三階段，於本點第二項先簡要說明該驗證機制於數位金融服務提供過程之運用情形，並附圖說明，嗣於第四點再詳予說明該三階段之作業程序。 三、 第三項定義數位身分驗證機制之六個參與者，惟不表示各參與者之角色必須由不同機構擔任，爰第四項說明金融服務業辦理數位身分驗證，依其組織架構及作業程序，可能同時擔任任一

（一） 客戶：身分驗證之標的。 （二） 註冊管理者：負責身分登錄相關作業(包括申請、身分核驗與身分資料驗證、註冊及紀錄留存)之權責單位。 （三） 信物服務提供者：負責管理信物生命週期以及建立並維持信物與身分資料間關聯性之權責單位。所稱信物係指一組數據之集合，可作為客戶所宣稱身分或權利之憑據，亦包含儲存信物之載體，例如晶片金融卡、證券商下單憑證及期貨商下單憑證等。 （四） 信賴者：信賴並使用身分驗證機制所得結果之單位。 （五） 驗證者：提供身分驗證服務之單位。 （六） 公正第三方：除註冊管理者、信物服務提供者、驗證者所提供之服務項目外，提供數位身分驗證機制所需其他服務而為前述參與者所信賴之單位。 金融服務業辦理數位身分驗證，依其組織架構及作業程序，可同時擔任註冊管理者、信物服務提供者、信賴者及驗證者等任一以上之參與者角色。	以上之參與者角色。 四、 第三項第六款所稱公正第三方，除包含身分資料之最終提供單位外，在核驗過程中協助資料傳遞與接收之單位亦屬之，故實務上如戶政機關、財金公司、票據交換所、金融聯合徵信中心、聯合信用卡處理中心、電信公司及憑證機構等均可能擔任公正第三方之角色。
四、 第三點第二項所定數位身分驗證機制三階段，原則上包含以下作業程序： （一） 身分登錄階段：(identity enrollment) 1. 身分核驗(identity proofing)：客戶提供身分資料(例如姓名、身分證、健保卡、信用卡、生物特徵、手機號碼、email 信箱、自然人憑證、數位簽章憑證、晶片金融卡、網路銀	一、 參考 ISO/IEC 29115，說明金融服務業辦理數位身分驗證包含三階段作業程序。其中於身分登錄階段之身分核驗程序，客戶所提供做為身分核驗之憑據，視為「身分資料」，例如自然人憑證、晶片金融卡或網路銀行帳號密碼等；而於信物管

行帳號密碼、電子支付帳戶帳號密碼、晶片護照等)，由註冊管理者就該身分資料進行核驗，核驗過程必要時應洽公正第三方提供資訊，以確認客戶身分資料之真實性、有效性及正確性。 2. 註冊及紀錄保存(registration and record-keeping)：註冊管理者將通過身分核驗之身分資料傳送予信物服務提供者，以辦理產製信物等後續作業。註冊管理者記錄並保存已蒐集的資料及檔案、身分資料核驗過程、決定(接受、拒絕或補件)及其他相關資訊。 (二) 信物管理階段：(credential management) 1. 綁定及核發(binding and issuance)：信物服務提供者完成信物產製程序後，將客戶、身分資料及信物三者間建立連結關係並進行綁定作業，再將信物核發予客戶。 2. 啟用及保存(activation and storage)：客戶收到信物後，依信物服務提供者之作業程序啟用信物，並應妥善保管，以避免未經授權者之使用。 3. 暫停、撤銷及更換(suspension, revocation and/or replacement)：信物服務提供者應依據信物使用情形及客戶狀態進行適當處理，例如信物之暫停、撤銷、更新或置換等措施。 (三) 身分驗證階段：(identity authentication)	理階段將客戶、身分資料及信物建立連結關係後，提供予客戶做為日後交易使用之憑據，視為「信物」，例如晶片金融卡、證券商下單憑證及期貨商下單憑證等。 二、 數位身分驗證機制原則上包含身分登錄、信物管理及身分驗證等三階段；其中於信物管理階段，視信物之特性，未必都會涉及信物之核發、啟用及保存等程序，例如客戶運用生物特徵做為數位身分驗證之信物，一般而言不會涉及信物之核發及啟用程序。 三、 為說明數位身分驗證機制各參與者之角色及功能，於第二項利用附圖二至五分別以晶片金融卡、證券商(期貨商)下單憑證、金融Fast-ID及保險公司網路會員帳號密碼或保險存摺帳號密碼做為信物等，舉例說明金融服務業之運作情形。又不同之信物管理機制，可能因金鑰保護能力(如晶片金融卡通過CC EAL4+認證)或憑證有效性驗證等差異，致信賴強度(即信賴等級)不同，所適用數位金融服務之應用場景亦應有所區隔。

1. 客戶及信物關聯性之驗證(authentication)：客戶向信賴者提出數位金融服務之需求並提示信物後，由信賴者向驗證者提出身分驗證之請求，驗證者依循信物服務提供者既定之身分驗證協定及客戶所提示信物，驗證客戶是否確實掌控並持有先前綁定之信物。 2. 驗證結果回復及紀錄保存(record-keeping)：驗證者於確認客戶確實掌控並持有信物後，依資料庫所登錄之信物與身分資料之關係，將驗證結果回復予信賴者，並留存相關驗證紀錄。 前項各參與者之角色及各階段之作業程序範例，詳參附圖二至附圖五。	
五、 金融服務業辦理數位身分驗證，其「應用場景之風險等級」與「驗證機制之信賴等級」應依風險基礎原則相互適配，並依以下評估作業辦理，金融服務業運用其他金融服務業之身分驗證機制提供數位金融服務者，亦同： (一) 數位身分驗證「應用場景之風險等級」評估作業：金融服務業應要求其業務單位於規劃數位金融服務之應用場景時，就身分驗證機制可能產生之風險進行評估，並評定所屬風險等級，做成「數位身分驗證應用場景之風險評估報告」。風險評估面向可包括該應用場景於採用之身分驗證機制失效時，可能造成客戶、公司營運、財務、名譽與法令遵循等風險。 (二) 數位身分「驗證機制之信賴等級」評	一、 參考 ISO/IEC 29115 及金融科技共創平台監理科技組之「多元之數位身分驗證」委託研究案，明定金融服務業辦理數位身分驗證，其「應用場景之風險等級」與「驗證機制之信賴等級」應依風險基礎原則相互適配。 二、 第一項第一款所稱「應用場景」係指金融服務業辦理之金融業務時之應用場景，因此不包含金融教育、金融測驗及內部作業等。 三、 第二項所稱現行法規、各業別自律規範及金融周邊單位相關規章對金融服務業辦理數位身分驗證已有規

估作業：金融服務業就各該應用場景之需求，針對可能採用之數位身分驗證機制進行信賴等級評估，並依身分登錄、信物管理及身分驗證等三階段，分別評估並得出整體綜合性之信賴等級，做成「數位身分驗證機制之信賴等級評估報告」。 （三） 適配「應用場景之風險等級」與「驗證機制之信賴等級」：金融服務業完成前兩項「數位身分驗證應用場景之風險評估報告」及「數位身分驗證機制之信賴等級評估報告」，於權衡其他因素(例如公司規模、成本、市場、複雜性及法律遵循等考量)後，就該「應用場景之風險等級」，依「驗證機制之信賴等級」選擇適當之身分驗證機制。 現行法規、各業別自律規範及金融周邊單位相關規章對金融服務業辦理客戶之數位身分驗證已有規範者，金融服務業免依前項規定辦理評估作業；現有規範未規定之新式數位金融服務應用場景或新式數位身分驗證方式，金融服務業除應依前項規定辦理評估作業外，開辦前並應洽詢主管機關是否須提出業務試辦之申請。	範者，詳如附件列表。
六、 第五點第一項第一款所稱應用場景採用之身分驗證機制失效時之可能風險包含： （一） 造成客戶不便、困擾。 （二） 造成客戶及金融服務業之名譽上損害。 （三） 造成客戶及金融服務業之財務損失或代理之責任。	一、 參考 ISO/IEC 29115，於第一項就數位金融服務應用場景所採用之數位身分驗證機制如失效時可能產生何種風險予以說明。 二、 第二項明定金融服務業應就第一項可能產生之風險及程度，區分等級，並以四

（四）對金融服務業、相關計畫或公共利益之損害。 （五）機敏資料未經授權公布。 （六）金融服務業違反相關法規。 金融服務業應評估前項各款之風險程度，並區分為不同等級，例如低、中、高及極高等四個風險等級。	個等級為例，惟並非只能區分為四個等級。 三、金融服務業評估第一項各款可能風險之等級後，應以其中最高之風險等級做為該應用場景之整體綜合性風險等級。例如 A 應用場景之身分驗證機制失效時，可能會產生第一項第一款之中風險等級、同項第二款低風險等級及同項第三款高風險等級，則 A 應用場景之整體綜合性風險等級應為高風險。
七、第五點第一項第二款所稱數位身分驗證機制之信賴等級係指對利用特定數位身分驗證機制驗證客戶所宣稱身分結果之可信程度。 金融服務業得依其業務性質，將前項信賴等級區分為不同級數。以區分為四個等級為例，各等級代表意義如下： （一）等級一：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；或於身分驗證失效時產生之風險屬低風險者，始可採用信賴等級一之數位身分驗證機制。 （二）等級二：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；或對於身分驗證失效產生之風險屬中風險者，至少應採用信賴等級二之數位身分驗證機制。 （三）等級三：對利用特定數位身分驗證	一、第一項參考 ISO/IEC 29115 及金融科技共創平台「多元之數位身分驗證」委託研究案，對數位身分驗證機制之信賴等級予以定義。 二、第二項明確揭示金融服務業可依其業務性質將信賴等級區分為不同級數。並參考 ISO/IEC 29115，以區分為四個等級為例，分別說明各等級代表之意義。 三、上述 ISO/IEC 29115 將數位身分驗證機制之信賴等級由低至高分為四個等級，僅是諸多分類方式的一種，且並非只能分為四個等級，例如美國國家標準與技術研究院(NIST)發布之數位身分驗證指南(Digital Identity Guidelines)係

機制所驗證客戶宣稱之身分有高度之信心；或對於身分驗證失效產生之風險屬高風險者，至少應採用信賴等級三之數位身分驗證機制。 （四） 等級四：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；或對於身分驗證失效產生之風險屬極高風險者，應採用信賴等級四之數位身分驗證機制。	將信賴等級分為低、中、高三個等級。 四、 金融服務業依身分登錄、信物管理及身分驗證三階段分別進行信賴等級評估時，如各階段得出之信賴等級不相同，應以最低之信賴等級做為該驗證機制之整體綜合性信賴等級。例如將信賴等級區分為四個等級時，B 身分驗證機制在身分登錄階段之信賴等級評估為等級三，在信物管理階段之信賴等級亦為等級三，但在身分驗證階段則為等級二，因此 B 身分驗證機制之整體綜合性信賴等級為等級二。再以前述 A 應用場景為例，A 應用場景之整體綜合性風險等級為高風險，而 B 身分驗證機制之整體綜合性信賴等級為等級二，因此 A、B 二者並不適配。
八、 金融服務業辦理數位身分驗證，應建立風險管理機制，並納入內部控制及稽核制度中，以有效保護客戶權益、防止詐欺及舞弊等。該風險管理機制應視業務及科技發展情況適時檢討。 前項風險管理機制，至少應包括下列事項： （一） 定期評估數位身分驗證機制之三階段作業程序及使用者(客戶、員工及第三方委外服務廠商等)使用金融服務系統過程中可能之風險、威脅	一、 第一項明定金融服務業辦理數位身分驗證應建立風險管理機制，並納入內部控制及稽核制度，且應視業務及科技發展情況適時檢討。 二、 第二項就金融服務業辦理數位身分驗證之風險管理機制，參考美國聯邦金融機構審查委員會(FFIEC)發布之「金融機構服務及系統之驗證及使用指南

及弱點，並評估身分驗證技術及管理機制是否足夠並加以檢討改進。前開評估內容應提出相關報告。 （二）採取適當措施以防範、監控、管理資通安全風險，包含防止篡改、身分盜用及資料濫用等保護措施，並訂定調查及處理已確認或可能之數位身分詐欺案件之作業程序。 （三）數位身分驗證如有涉及其他機構，應釐清相關風險與責任，並視必要性及可行性約定雙方之權利義務。 （四）建立受理客戶申訴、爭議處理及補救之內部標準程序，包括身分驗證機制失誤、發生未經授權交易等情形之通報、處理及補救措施，避免客戶使用數位金融服務之權利因此受損，以及避免問題擴大致影響金融服務業之正常營運。 （五）對辦理數位身分驗證之員工應施以相關教育訓練，內容至少應包括與身分驗證相關之法規、技術、作業程序、風險辨識及因應措施，以及客戶權益保護等。 （六）建立營運持續及事件復原計畫，提升數位身分驗證機制之可靠性。	(Authentication and Access to Financial Institution Services and Systems)」、澳洲之可信任數位身分框架(Trusted Digital Identity Framework Accreditation Rule)」及OECD之「電子驗證指南(OECD Guidance for Electronic Authentication)」等規範，列舉至少應包括之事項，例如定期評估、使用金融服務系統之管理、數位身分詐欺控管機制、客戶爭議處理之內部標準程序、員工教育訓練、營運持續及事件復原計畫等。
九、 金融服務業辦理數位身分驗證，應注意以下與客戶權益有關事項： （一）就客戶是否加入金融服務業建立之數位身分驗證機制，應由客戶自主決定。金融服務業並應提供多元管道，以利客戶親至實體營業場所或透過行動裝置、網際網路等遠距模式完成身分驗證程序。 （二）就取得之個人資料，告知客戶得撤	明定金融服務業辦理數位身分驗證，應注意與客戶權益有關之事項，包括由客戶自主決定是否加入數位身分驗證機制、提供多元管道供客戶完成身分驗證、客戶撤回或修正其同意蒐集處理利用個人資料之方式，以及提供客戶安全認知教育宣導等。其中第三款有關客戶安全認知教育

回或修正其已表示同意蒐集、處理及利用之方式。 （三）提供客戶安全認知教育宣導，並定期更新宣導內容以反映外在風險之變化，內容至少應包括如何保護客戶自身之數位身分、個人資料及信物、如何確認取得金融服務之合法溝通管道(如官方網址)、可用以降低風險之控制措施(如金融服務業採多因子驗證機制之理由、設定網路交易限額)、常見外部威脅(如社交工程、釣魚網站)，以及發生未經授權交易時，客戶可能擁有之法律及其他權利保護等。	宣導，金融服務業可於其官方網站提供相關資訊。
十、 金融服務業各產業公會及金融周邊單位得參考本指引訂定數位身分驗證作業程序及評估作業，並給予個別金融服務業者自行訂定內部規範之彈性。	參考金融科技共創平台「多元之數位身分驗證」委託研究案，明定金融服務業各產業公會及金融周邊單位於訂定數位身分驗證作業程序及評估作業，允宜給予個別金融服務業者自行訂定內部規範之彈性，俾各該業者依其業務發展情形妥適因應相關風險。