保險業辦理數位身分驗證自律規範

金融監督管理委員會 114.12.09 金管保綜字第 1140419731 號函同意備查

第一條 制定目的

為協助保險業使用數位身分驗證機制時建立有效的安全驗證機制，同時提供民眾便利、快速、安全之數位金融服務，並協助保險業運用適當之數位身分驗證機制以降低潛在之風險，特訂定本自律規範。

第二條 用詞定義及說明

本自律規範用詞定義及說明：

一、數位身分驗證(Digital Identity Authentication)係指於數位金融環境利用適當之技術與機制，確認客戶為其所宣稱身分之過程。

(一)數位身分驗證機制參與者定義：

1. 客戶：身分驗證之標的(客戶以自然人為限)。
2. 註冊管理者：負責客戶身分登錄相關作業(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。
3. 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，例如晶片金融卡等。
4. 信賴者：信賴並使用身分驗證機制所得結果之單位。
5. 驗證者：提供身分驗證服務之單位。
6. 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。

二、多因子驗證(Multi-Factor Authentication, MFA)：是一種安全措施，要求客戶在進行身分驗證時提供兩種或以上不同類型的認證因子，包括知識因子、生物特徵因子，以及持有因子。目的是提供比單一認證方式更高的安全層級，通過要求多種驗證使用者的身分，從而增加未經授權存取成功的安全難度。

三、C3 憑證：係指符合我國電子簽章法之臺灣網路認證公司簽發第三級商務 EC+憑證、第三級商務 XML 憑證(含商務 XML Plus)或中華電信公司簽發第三級 Public CA 憑證，其註冊中心應為金融機構。

四、信賴等級機制：係參考 ISO 29115 框架與遵循「金融服務業辦理數位身分驗證指引」第七點以身分登錄、信物管理、身分驗證三個面向，依據安全設計與風險區分為極高、高、中、低四個信賴等級。

第三條 數位身分驗證機制

數位身分驗證機制包含三個階段：「身分登錄」、「信物管理」及「身分驗證」，客戶於首次啟用保險業數位金融服務時，各會員公司應透過「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，且應就身分驗證階段進行核驗，其中身分登錄及信物管理階段視作業程序特性，若會員公司未涉及該作業程序(例如信用卡驗證信物管理方為信用卡發卡方)，或會員公司角色為信賴者，則可屬不適用範圍。

一、身分登錄階段：

(一)身分核驗：客戶提供身分資料(例如姓名、身分證、健保卡等足以識別身分之資料)，應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。

(二)註冊及紀錄保存：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。

(三)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：

(一)綁定及核發：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。

(二)啟用及保存：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。

(三)暫停、撤銷及更換：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：

(一)客戶及信物關聯性之驗證：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。

(二)驗證結果回復及紀錄保存：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。

第四條 第三方認證方式

各會員公司提供客戶辦理身分驗證作業，得依主管機關核准或與客戶線上約定之身分驗證程序或數位憑證辦理；有關主管機關核准之第三方認證方式如下：

一、內政部核發之自然人憑證與行動自然人憑證。

二、網路銀行帳戶(以銀行臨櫃辦理者為限)或數位存款帳戶(適用電子轉帳交易指示類高風險交易之第一類帳戶)。

三、金融機構或主管機關認可核發之金融憑證。

四、金融行動身分識別聯盟之「金融行動身分識別標準化機制」(金融Fast-ID)。

五、行動身分識別(Mobile ID)應由經過第三方認證機構向手機門號所屬之電信業者進行身分驗證。

六、除前述規定之認證方式外，於其他法令、主管機關已核准方式或相關函釋另有規定者，從其規定。

第五條 風險基礎原則適配性

各會員公司辦理數位身分驗證，應遵循「金融服務業辦理數位身分驗證指引」第五點之風險基礎原則相互適配性，依要求制定其「應用場景之風險等級」與「驗證機制之信賴等級」。

第六條 身分驗證機制失效時之可能風險

各會員公司應評估身分驗證機制失效時之可能風險，並依據風險制定對應之控制措施，

其風險包含：

一、造成客戶不便、困擾。

二、造成客戶及會員公司之名譽上損害。

三、造成客戶及會員公司之財務損失或代理之責任。

四、對會員公司、相關計畫或公共利益之損害。

五、機敏資料未經授權公布。

六、會員公司違反相關法規。

各會員公司應評估前項各款可能之風險與衝擊程度，並將整體綜合性風險等級區分為低、中、高、極高風險。

第七條 信賴等級設計原則

各會員公司應依「金融服務業辦理數位身分驗證指引」第五點第一項第二款所稱之數位身分驗證機制之信賴等級，依其業務性質，將信賴等級區分為不同級數，各信賴等級定義如下：

一、等級一之低信賴等級：本等級定義為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度風險者，始可採用信賴等級一之數位身分驗證機制。會員公司採取本等級應考量建立身分核驗機制、存取資料之風險、基本驗證機制之有效性等。

二、等級二之中信賴等級：本等級定義為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度風險者，至少應採用信賴等級二之數位身分驗證機制。等級二至少具有一項身分登錄、持有一種信物，以及安全的身分驗證方式，會員公司如採用不同因子安全設計使其成為多因子驗證機制，則可依第八條說明以提升信賴等級。

三、等級三之高信賴等級：本等級定義為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；或對於身分驗證失效產生之風險屬高度風險者，至少應採用信賴等級三之數位身分驗證機制，等級三為本自律規範次高等級之認證機制，管理機制應至少採用多因子驗證機制，且身分驗證過程的機敏資料傳輸與儲存均應加密保護。

四、等級四之極高信賴等級：本等級定義為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度風險者，應採用信賴等級四之數位身分驗證機制。等級四為本自律規範最高等級的認證機制，需基於等級三之作業內容，並於身分登錄時應採面對面或使用具有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私鑰，所有機敏資料傳輸與靜態保存時應採加密保護。如會員公司採網路視訊軟體核驗身分，應留存政府核發用於身分識別之證件(如國民身分證、居留證或護照等)之影像檔；若客戶為本國籍未成年人，則應增加核驗其法定代理人之上述證明文件。

前項數位身分驗證機制之信賴等級詳如附表一。

第八條 身分核驗安全設計及信賴等級對應機制

單一使用視訊驗證機制為信賴等級三之高信賴等級；其餘各類別所列之任一因子單獨使用時為信賴等級二之中信賴等級。

第一類知識因子信賴等級對應機制包含下列身分核驗安全設計：

一、固定密碼。

二、圖形鎖或手勢。
三、銀行存款帳號驗證。
四、保險存摺帳號密碼。
五、國民身分證領補換發。
第二類生物特徵因子信賴等級對應機制包含下列身分核驗安全設計：
一、直接生物辨識。
二、間接生物辨識。
第三類持有因子信賴等級對應機制包含下列身分核驗安全設計：
一、金融行動身分識別標準化機制。
二、一次性密碼。
三、行動身分識別(Mobile ID)。
四、金融憑證。
五、客戶約定之設備。
六、信用卡驗證。
七、晶片金融卡。
八、自然人憑證。
第四類多因子信賴等級對應機制之身分核驗安全設計：視訊驗證機制。
各會員公司採用第二項至第五項所定第一類至第四類對應機制之身分核驗安全設計時,,應建立連線(Session)控制及網頁逾時(TimeOut)中斷機制，當客戶逾時於一定限制時間內未進行任何操作時系統應自動中斷連線，並透過不同身分核驗安全設計配合，分別可達到之信賴等級如下：
一、除第一類對應機制之身分核驗安全設計不得互用外，如第一類至第三類對應機制之身分核驗安全設計互相配合；或逕採用其他主管機關核准方式等擇一方式時，可達等級三之高信賴等級，下列第二款除外。
二、第三類身分核驗安全設計之晶片金融卡或自然人憑證，並配合第一類至第四類任一身分核驗安全設計；或逕採用前款以外之其他主管機關核准方式或者，可達等級四之極高信賴等級。
除前項機制,各會員公司得採行符合第七條第一項第二款至第四款之身分核驗安全設計,可達等級二至等級四之信賴等級。
當原先身分驗證階段驗證機制信賴等級低於後續應用服務之風險場景者，應於同一連線及有效工作階段內，遵循本規範第八條第二項至第五項規定，補足以達成相應信賴等級之身分驗證機制，以確保應用場景之風險等級與驗證機制之信賴等級相互適配性；若同一連線及有效工作階段內，身分驗證階段驗證機制信賴等級高於或等於後續應用服務之風險場景者，則無須再次驗證。
本條身分核驗安全設計及信賴等級對應機制詳如附表二。

第九條 固定密碼
安全設計應符合下列要求：
一、身分登錄：
身分登錄依下列三項申請方式擇一。
(一)客戶於會員公司臨櫃申請，經身分核驗後，由會員公司完成身分登錄，並取得帳號與密碼。

(二)客戶依主管機關核可之方式，或於會員公司系統經身分核驗程序後完成身分登錄，取得固定密碼；由客戶取得帳號及自行設定密碼者同。

(三)帳號可由客戶自行設定或選擇使用「身分證統一證號」、「外來人口統一證號」、「護照號碼」作為帳號。

二、信物管理：

(一)應至少八位數。

(二)應採英數字混合使用，且宜包含大小寫英文字母或符號。

(三)不得使用客戶之國民身分證統一編號顯性資料作為密碼。

(四)不應訂為連續三碼以上相同的英數字、連續英文字或連號數字，預設密碼不在此限。

(五)密碼與帳號不應相同。

(六)密碼連續錯誤達五次，各會員公司應做妥善處理。

(七)變更密碼時應核驗原密碼且不得與前一次相同。

(八)若密碼為會員公司提供，首次登入時應強制變更預設密碼，若未於 30 日內變更者，則不得再以該密碼執行登入。

(九)密碼超過一年未變更，各會員公司應妥善提醒客戶密碼變更事宜。

(十)應採用下列一項密碼儲存管控機制：

1. 密碼於儲存時應先進行不可逆運算(如雜湊演算法)，雜湊值應進行加密保護或加入不可得知的資料運算。

2. 採用加密演算法者，其金鑰應儲存於軟體式金鑰管理器並與原資料庫區隔，或搭配經第三方認證(如 FIPS 140-2 Level 3 以上)之硬體安全模組並限制明文匯出功能等。

(十一)當進行密碼重設機制(如忘記密碼)時，應確認使用者身分，得發送一次性及具有時效性符記，以加強防護機制(如交易密碼驗證、設備指定、推播確認、遞延交易並可偵測阻擋、OTP 綁交易、語音 OTP、SIM 卡認證、錄影存證、雙向簡訊並可辨識來源電話、或依會員公司風險評估至少具相同安全強度之安全機制，並應留存評估紀錄及核決層級)，且該機制應排除靜態密碼認證。

三、身分驗證：

(一)應核驗與客戶所約定之密碼。

(二)針對密碼與傳輸通道應採取適當的加密機制。

第十條 圖形鎖或手勢

安全設計應符合下列要求：

一、身分登錄：

限以客戶於會員公司申請約定後完成啓用，或完成身分登錄並核發固定密碼者於行動應用程式(APP)啟用者為限。

二、信物管理：

(十二) 連續錯誤達五次，各會員公司應做妥善處理。

(十三) 變更不得與前一次相同。

三、身分驗證：

(一)客戶與會員公司所約定之資訊，且無第三人知悉之圖形鎖或手勢。

(二)採用圖形鎖或手勢技術者，宜事先評估客戶身分驗證機制之有效性，善盡告知客

戶使用上之風險，並提供驗證機制關閉管道。

第十一條 銀行存款帳號驗證

安全設計應符合下列要求：

一、身分登錄：

客戶於銀行臨櫃開戶或符合數位存款帳戶(適用電子轉帳交易指示類高風險交易之第一類帳戶)標準，經身分核驗後，由銀行完成身分登錄，並取得網路銀行帳號與密碼。

二、信物管理：

不適用。

三、身分驗證：

(一)確認客戶與該帳戶持有人為同一國民身分證統一編號且係透過臨櫃方式開立或符合數位存款帳戶(適用電子轉帳交易指示類高風險交易之第一類帳戶)標準，以確認該帳戶之有效性。

(二)會員公司向其存款帳戶銀行提出對客戶進行身分驗證之請求，透過該銀行驗證後，會員公司僅讀取該銀行回復驗證結果。

(三)身分驗證得透過公正第三方機構進行跨機構核驗。

第十二條 保險存摺帳號密碼

安全設計應符合下列要求：

一、身分登錄：

客戶應於壽險公會官網保險存摺專區登錄與完成核驗身分後辦理。

二、信物管理：

(一)壽險公會應留存相關申請紀錄、資料傳輸與接收軌跡紀錄。

(二)資料及檔案之傳輸與儲存，應依主管機關要求之資訊安全防護相關規範辦理。

(三)針對所傳輸之個人資料，會員公司應建置適當之保護設備或技術，採取適當之存取管制。

三、身分驗證：

(一)確認客戶與保險存摺持有人為同一國民身分證統一編號，以確認該帳戶之有效性。

(二)須為保險存摺之白金會員後，始能透過保險存摺帳密進行驗證。

第十三條 國民身分證領補換

安全設計應符合下列要求：

一、身分登錄：

依據「戶籍法」對於中華民國國民身分證申請人資格等規範，至戶政事務所申辦初領、補領、換領中華民國國民身分證。

二、信物管理：

不適用。

三、身分驗證：

(一)依據身分證之發證資訊，包含國民身分證統一編號、發證類型、發證日期、發證地點等欄位資訊，進行向內政部戶政司身分證領補換發資料驗證程序，會員公司僅讀取內政部回復驗證結果。

(二)身分驗證得透過公正第三方機構進行跨機構核驗。

(三)針對傳輸通道應採取適當的加密機制。

第十四條 直接生物辨識

安全設計應符合下列要求：

一、身分登錄：

身分登錄依下列兩項申請方式擇一。

(一)客戶依會員公司申辦流程臨櫃、親晤或網路視訊軟體辦理。

(二)客戶於會員公司系統、公正第三方機構或依主管機關核可之方式進行身分核驗，經會員公司之身分核驗程序結合生物特徵完成後，由會員公司完成身分登錄。

二、信物管理：

依保險業辦理資訊安全防護自律規範附件三保險業運用新興科技作業原則之伍、生物特徵資料安全控管條款辦理。

三、身分驗證：

(一)客戶提供給會員公司其所擁有之生物特徵，會員公司應直接驗證該生物特徵。

(二)採用直接驗證生物特徵技術者，應確認真人及本人辦理並符合保險業辦理資訊安全防護自律規範附件三保險業運用新興科技作業原則之伍有關生物特徵資料安全控管要求。

第十五條 間接生物辨識

安全設計應符合下列要求：

一、身分登錄：

客戶於會員公司申請約定後於支援裝置完成啟用。

二、信物管理：

不適用。

三、身分驗證：

(一)間接驗證係指由客戶端設備(如行動裝置)驗證或委由第三方驗證，會員公司僅讀取回復驗證結果，必要時應增加驗證來源辨識。

(二)採用間接驗證生物特徵技術者，宜先評估客戶身分驗證機制之有效性，善盡告知客戶使用上之風險，並提供驗證機制關閉管道。

(三)身分驗證得透過公正第三方機構進行跨機構核驗。

第十六條 金融行動身分識別標準化機制

安全設計應符合下列要求：

一、身分登錄：

客戶於金融機構首次申辦，經身分核驗後，由金融機構完成身分登錄，並在客戶設備內進行生物特徵設定或綁定、產生 FIDO 金鑰對、私鑰妥善儲存於客戶設備內及公鑰儲存於金融機構之FIDO伺服器。

二、信物管理：

應遵循「金融機構辦理快速身分識別機制安全控管作業指引」第三點與第四點之要求，核驗身分後辦理註冊與信物管理作業。

三、身分驗證：

應採用客戶所指定之設備及其生物特徵進行FIDO驗證與遵循「金融機構辦理快速身

分識別機制安全控管作業指引」第五點之要求。

第十七條 一次性密碼

安全設計應符合下列要求：

一、身分登錄：

由客戶提供或自行輸入之帳號及密碼或個人識別資料(如國民身分證統一編號、出生年月日等)後完成身分登錄辦理，會員公司依與客戶約定發送一次性密碼之手機門號或電子信箱。

二、信物管理：

(一)應至少六位數。

(二)輸入密碼連續錯誤達五次，該密碼即失效。

(三)每次密碼有效性不得逾5分鐘，逾時即需重新申請發給新密碼。

(四)手機號碼或電子信箱之異動： 會員公司應核驗客戶身分後重新設定。

(五)採用簡訊傳輸一次性密碼發送端之電話門號應與發送行銷廣告之門號有所區隔，以利客戶識別。如採用商用簡碼者，則不在此限。

三、身分驗證：

應運用一次性密碼技術產生並限制一次性使用。

第十八條 行動身分識別(Mobile ID)

安全設計應符合下列要求：

一、身分登錄：

應由客戶臨櫃或線上至電信業者申辦之門號，申辦程序應依電信事業受理電信服務相關規範辦理。

二、信物管理：

(一) 客戶申辦之門號限月租型門號，應排除儲值卡、親子卡、預付卡、企業卡等門號。

(二)會員公司應留存客戶完成Mobile ID驗證使用之相關軌跡紀錄。

三、身分驗證：

(一)客戶宜先閱讀同意第三方公正機構驗證所公告之使用者約定條款及隱私權告知相關條款。

(二)經客戶同意，透過第三方公正機構驗證客戶與該門號租用人為同一國民身分證統一編號。若係透過用戶身分模組（Subscriber Identity Module，SIM）連線至該電信業者，則應另確認該SIM之有效性，會員公司僅讀取電信業者回復驗證結果。

(三)資料及檔案之傳輸與儲存，應依主管機關要求之資訊安全防護相關規範辦理。

(四)身分驗證得透過公正第三方機構進行跨機構核驗。

(五)針對所傳輸之個人資料，會員公司應建置適當之保護設備或技術，採取適當之存取管制。

第十九條 金融憑證

安全設計應符合下列要求：

一、身分登錄：

客戶於金融機構申辦，經身分核驗後，由金融機構完成身分登錄後，核發客戶之金

融憑證(如證券商期貨商下單憑證)。

二、信物管理：

(一)應採用符合註冊中心為金融機構之金融憑證(如金融 XML 憑證、C3 憑證或非對稱性加解密系統)。

(二)私鑰應經密碼保護，以確保金鑰儲存安全。

三、身分驗證：

(一) 會員公司向金融機構提出對客戶進行身分驗證之請求，確認憑證簽章有效性及正確性後，會員公司僅讀取憑證金融機構回復驗證結果。

(二) 身分驗證得透過公正第三方機構進行跨機構核驗。

第二十條 客戶約定之設備

安全設計應符合下列要求：

一、身分登錄：

客戶於會員公司申請約定，會員公司經確認客戶身分後進行身分驗證之設備。

二、信物管理：

(一)客戶與會員公司所約定持有之設備包含但不限於行動裝置、密碼產生器、密碼卡、晶片卡、電腦、憑證載具、SIM 卡認證等。

(二)客戶約定之設備應透過安全軟體授權後運行。

三、身分驗證：

會員公司應確認該設備為客戶與會員公司所約定持有之實體設備，透過會員公司驗證該裝置為同一個人國民身分證統一編號後，由會員公司回復驗證結果。

第二十一條 信用卡驗證

安全設計應符合下列要求：

一、身分登錄：

客戶於金融機構申辦，經身分核驗後，由金融機構完成身分登錄後，核發客戶之信用卡。

二、信物管理：

不適用。

三、身分驗證：

(一)確認申請人與信用卡持卡人為同一個人國民身分證統一編號且係透過信用卡授權交易方式，以確認該卡片之有效性(如預授權)。

(二)驗證金融機構信用卡有效性時，應透過聯合信用卡處理中心及財金公司之「信用卡輔助持卡人身分驗證平臺」及其他合作銀行或電子支付機構辦理，會員公司僅讀取發卡銀行回復驗證結果。

(三)身分驗證得透過公正第三方機構進行跨機構核驗。

第二十二條 晶片金融卡

安全設計應符合下列要求：

一、身分登錄：

客戶於銀行臨櫃開戶或符合數位存款帳戶(適用電子轉帳交易指示類高風險交易之第一類帳戶)標準，經身分核驗後，由銀行完成身分登錄，並提供晶片金融卡。

二、信物管理：

不適用。

三、身分驗證：

會員公司向發卡銀行提出對客戶進行身分驗證之請求，透過發卡銀行驗證客戶與該晶片金融卡帳號為同一個人國民身分證統一編號後，會員公司僅讀取發卡銀行回復驗證結果。

第二十三條 自然人憑證

安全設計應符合下列要求：

一、身分登錄：

身分登錄依下列兩項申請方式擇一。

(一)客戶於戶政事務所臨櫃申辦，經身分核驗後，由戶政事務所核發之晶片自然人憑證。

(二)客戶於內政部網頁申請，經身分核驗程序並核發及裝置綁定後，由內政部完成身分登錄，啟用行動自然人憑證服務。

二、信物管理：

不適用。

三、身分驗證：

(一)會員公司向內政部提出對客戶進行身分驗證之請求，確認憑證簽章有效性及正確性後，會員公司僅讀取憑證機構回復驗證結果。

(二)身分驗證得透過公正第三方機構進行核驗。

第二十四條 視訊驗證

安全設計應符合下列要求：

一、身分登錄：

不適用。

二、信物管理：

留有客戶身分識別之證件(如國民身分證、居留證或護照等)影音檔應有加密傳輸與儲存之安全防護機制。

三、身分驗證：

(一)應請客戶出示政府核發用於身分識別之證件(如國民身分證、居留證或護照等)，比對客戶本人樣貌與證件照片之一致性。但無國民身分證之未成年者，應出示附有照片之健保卡或護照。

(二)應導入機制協助確認真人及本人，以防止透過科技預先錄製影片、製作面具、模擬影像或深度偽造(deepfake)等機制偽冒身分。

(三)應建立身分證明文件偵錯防偽，或向發證機關查詢確認其真偽之機制並進行驗證；若客戶係本國籍未成年人，應增加核驗其法定代理人之上述證明文件。

第二十五條 風險管理機制

各會員公司風險管理機制應遵循「金融服務業辦理數位身分驗證指引」第八點之要求建立風險管理機制，並納入內部控制及稽核制度，該風險管理機制應視業務及科技發展情況適時檢討。

第二十六條 罰則

各會員公司如有違反本自律規範之情事，經查證屬實者且違反情節較輕者，得先予書面

糾正；如情節較重大者，提報經各所屬公會理事會通過後，處以新台幣伍萬元以上，貳拾萬元以下之罰款；前述處理情形並應於一個月內報主管機關。

第二十七條 客戶權益

應遵循「金融服務業辦理數位身分驗證指引」第九點之客戶權益有關事項，應開放客戶自主決定是否加入由會員公司建立之數位身分驗證機制。

會員公司並應提供多元管道，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，並保障客戶使用數位身分驗證機制。

第二十八條 施行程序

本規範由中華民國人壽保險商業同業公會與中華民國產物保險商業同業公會共同訂定，經各該公會理(監)事會決議通過報請主管機關備查後施行，修正時亦同。

本自律規範自 115 年 1 月 1 日起實施，會員公司之相關調整作業，應於實施日期前完成調整。

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； • 對於身分驗證失效產生之風險屬極高風險者。	• 客戶需面對面進行身分登錄，確保身分真實性。 • 客戶本人親自與會員公司採面對面方式完成身分登錄。	• 所有金鑰需儲存在防篡改硬體中。 • 敏感資料需在傳輸和儲存中全面加密保護。	• 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構的身分資訊進行驗證。 • 進行身分真實性資訊確認。	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。

附表二、 身分核驗安全設計及信賴等級對應機制表

<table>
<tr><th>類別</th><th>單獨使用</th><th>搭配使用</th></tr>
<tr><td>第一類知識因子：
一、固定密碼
二、圖形鎖或手勢
三、銀行存款帳號驗證
四、保險存摺帳號密碼
五、國民身分證領補換發</td><td>信賴等級二之中信賴等級</td><td rowspan="4">各會員公司採用第八條第二項至第五項所定第一類至第四類對應機制之身分核驗安全設計時，應建立連線(Session)控制及網頁逾時(TimeOut)中斷機制，當客戶逾時於一定限制時間內未進行任何操作時系統應自動中斷連線，並透過不同身分核驗安全設計配合，分別可達到之信賴等級如下：
1. 除第一類對應機制之身分核驗安全設計不得互用外，如第一類至第三類對應機制之身分核驗安全設計互相配合；或逕採用其他主管機關核准方式等擇一方式時，可達等級三之高信賴等級，下列第二款除外。
2. 第三類身分核驗安全設計之晶片金融卡或自然人憑證，如配合第一類至第四類任一身分核驗安全設計；或逕採用前款以外之其他主管機關核准方式者，可達等級四之極高信賴等級。
除前項機制，各會員公司得採行符合第七條第一項第二款至第四款之身分核驗安全設計，可達等級二至等級四之信賴等級。
當原先身分驗證階段驗證機制信賴等級低於後續應用服務之風險場景者，應於同一連線及有效工作階段內，遵循本規範第八條第二項至第五項規定，補足以達成相應信賴等級之身分驗證機制，以確保應用場景之風險等級與驗證機制之信賴等級相互適配性；若同一連線及有效工作階段內，身分驗證階段驗證機制信賴等級高於或等於後續應用服務之風險場景者，則無須再次驗證。</td></tr>
<tr><td>第二類生物特徵因子：
一、直接生物辨識
二、間接生物辨識</td><td>信賴等級二之中信賴等級</td></tr>
<tr><td>第三類持有因子：
一、金融行動身分識別標準化機制(金融Fast-ID)
二、一次性密碼
三、行動身分識別(Mobile ID)
四、金融憑證
五、客戶約定之設備
六、信用卡驗證
七、晶片金融卡
八、自然人憑證</td><td>信賴等級二之中信賴等級</td></tr>
<tr><td>第四類多因子：視訊驗證機制</td><td>等級三之高信賴等級</td></tr>
</table>