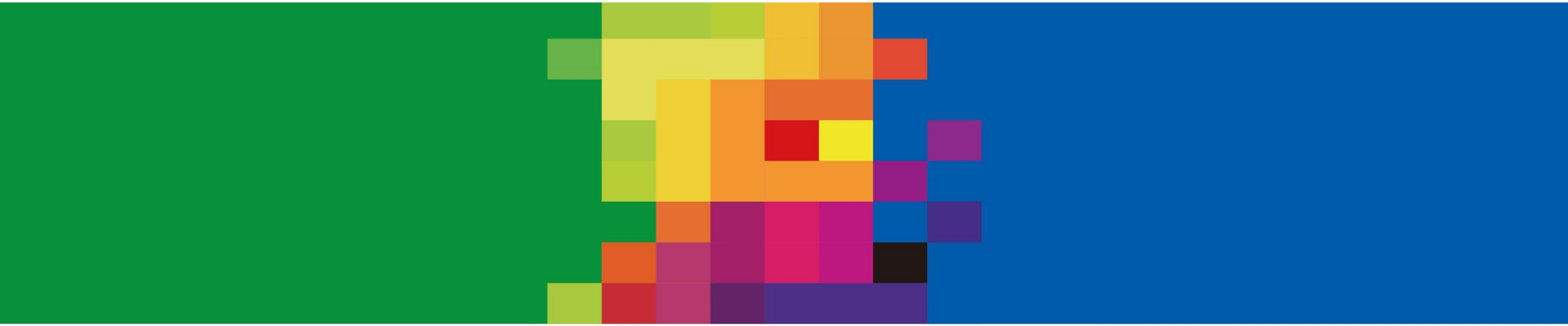
證券商資訊主管業務座談會
電子簽章創新服務生態圈實務分析

臺灣網路認證公司
連子清 協理



TWCA 臺灣網路認證

TWID 身分識別中心

簡報大綱

- 背景
- 電子簽章法修正要點
- 證券期貨線上服務身分驗證
- ISO 29115 個體驗證信賴框架及定義

背景說明

電子簽章法修訂

- 《電子簽章法》(113.5.15)，明定數位簽章有「**推定**」為本人親簽或蓋章的效力
- 《數位簽章憑證實務作業基準應載明事項》，要求憑證用戶初始註冊身分識別與認證程序之保證等級強度 (身分識別強度) 至少須達**保證等級三** (ISO/IEC 29115)

金管會要求線上身分識別框架參考 ISO 29115

- **銀行** 委外修訂《電子銀行業務安全控管作業基準》(進行中)
- **證券/期貨** 由公會委外彙整線上服務的身分驗證實務作業指引 (進行中)
- **保險** 已提出《保險業辦理數位身分驗證自律規範》(草案已公佈)

電子簽章法修正要點

電子簽章法修正重點

1. 明示電子與紙本具同等功能

- **鑒於以往大眾對書面文件及簽章改採電子形式之效力，常有疑慮**，明訂「電子文件、電子簽章」不得僅因其電子形式而否認其法律效力。
- 參酌聯合國貿易法委員會電子商務模範法、美國聯邦全球與國家商務電子簽章法、韓國電子簽章法、歐盟內部市場電子身分識別與可信賴電子交易服務規則(eIDAS Regulation)等國際法例，增列條文明示電子與紙本具同等功能。

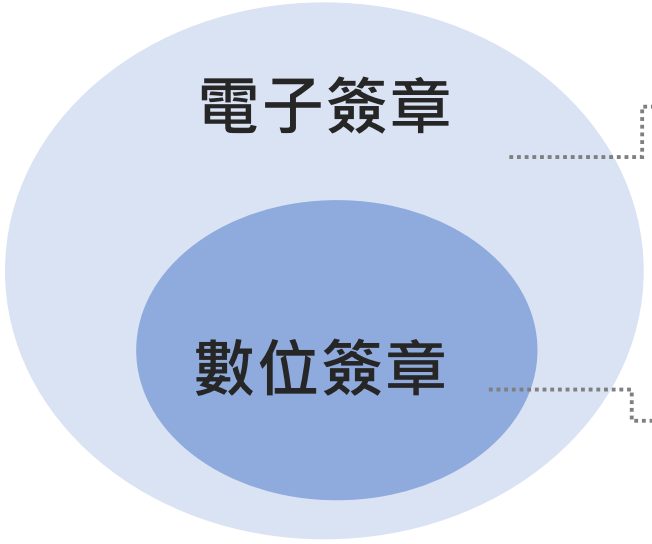
新增條文第4條

電子文件及電子簽章，符合本法規定者，在功能上等同於實體文件及簽章，不得僅因其電子形式而否認其法律效力。

電子簽章法修正重點

2. 電子簽章與數位簽章關係明確化

- 「**數位簽章**」符合電子簽章之定義，但數位簽章使用經主管機關許可之憑證機構所簽發之憑證，運用了演算法和加密技術，多了一道驗證手續。
- 「電子簽章」如同傳統紙本時代的便章。
- 「數位簽章」使用憑證機構簽發憑證，該憑證如同傳統紙本時代的印鑑證明。



修正條文第2條第2款

- 定義：指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。

修正條文第2條第3款

- 定義：**屬於電子簽章之一種，**指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，得以公開金鑰加以驗證，**並具憑證機構簽發之憑證者。**

電子簽章法修正重點

3. 經憑證機構核發憑證產生的數位簽章，具推定本人親自簽名或蓋章之效力

- 數位簽章為實務上常用之電子簽章，因能連結及識別簽名人、偵測簽名所依附文件之改變，且具憑證機構簽發之憑證，具一定程度公信力。
- 數位簽章在訴訟上舉證所具有的證據力與未具憑證機構簽發憑證之電子簽章有別，爰修正具備憑證機構所簽發憑證之數位簽章具有「推定」為推定為本人親自簽名或蓋章之效力。

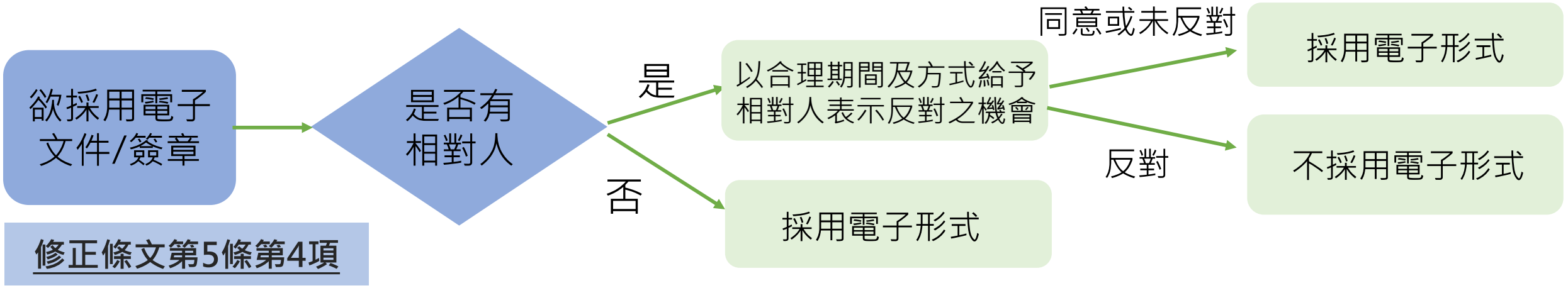
修正條文第6條

效力：推定為本人親自簽名或蓋章
(有更強的證據力)

電子簽章法修正重點

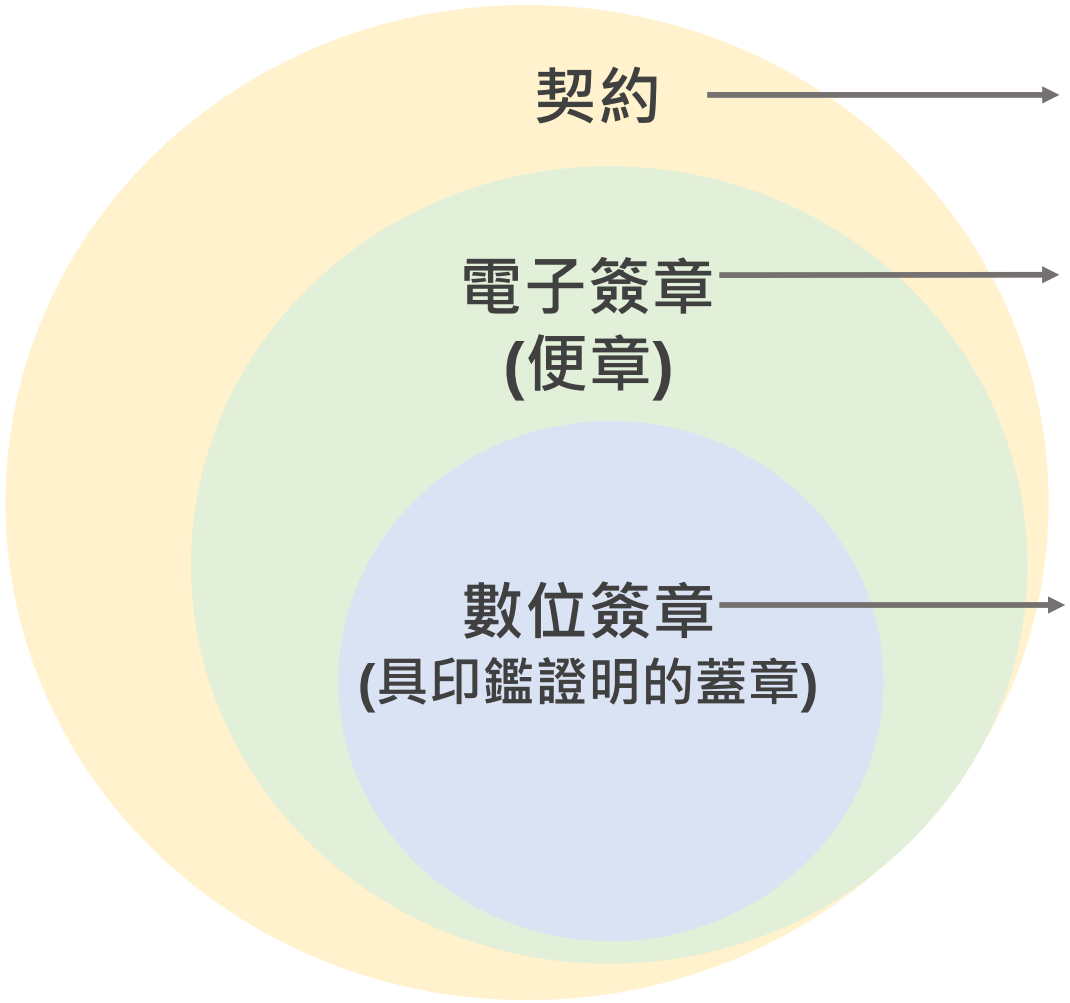
4. 調整經相對人同意之要件

- 實務使用電子文件或電子簽章，**不一定有相對人**，不宜將「經相對人同意」作為**所有**電子文件或電子簽章之使用前提
- 兼顧數位化需求與社會包容，考量相對人有**數位落差**可能性，爰增訂第四項規定，於有相對人之法律行為，除相對人已同意採用電子形式外，**應於採用電子形式之前，以合理期間及方式給予相對人反對之機會；並告知相對人未反對者，推定同意採用電子形式。**



修正條文第5條第4項

電子簽章法規定義



民法第 153 條

當事人互相表示意思一致者，
無論其為明示或默示，契約即為成立。

當事人對於必要之點，意思一致，而對於非必要之點，未經表示意思者，推定其契約為成立，關於該非必要之點，當事人意思不一致時，法院應依其事件之性質定之。

需符合電子簽章法中的完備三要素

1.依附於電子文件並與其相關連
2.辨識及確認電子文件簽署人身分、資格
3.辨識電子文件真偽者。

透過憑證機構核發憑證產生的數位簽章可以推定為本人親自簽名或蓋章。

1. 將電子文件以數學演算法或其他方式運算為一定長度之數位資料
2. 以簽署人之私密金鑰對其加密，形成電子簽章，得以公開金鑰加以驗證辨識電子文件真偽者。
3. 並具憑證機構簽發之憑證者

紙本契約書 v.s. 電子契約書

紙本契約書

契約書

印章

印鑑 (或印樣)

印鑑登錄證明書

印鑑比對

將合約書上的印鑑和印鑑登記證明書上的印鑑進行對比，用人眼進行核對

當事人使用數位簽章產生電子契約

具備數位簽章的契約書 PDF 檔案

用於數位簽章的私密金鑰 (簡稱私鑰)

數位簽章 (一組利用私鑰對契約書內容運算產生的數據)

電子憑證

簽章驗證

利用數位簽章和電子憑證中包含的資料及公鑰，用軟體自動進行對比。

「證券暨期貨業者線上服務身分驗證實務作業參考」委託專案
專案背景

證交所規劃研擬修訂安控基準及新版電子簽章法明定政府於修法實施一年後，排除原停止適用電子簽章法之行政公告，影響證券及期貨業電子化業務。

電子簽章法因應

針對證券商暨期貨商線上服務項目彙整表等議題，依風險基礎原則，與第三方專家合作提出業務風險等級評估。

業務風險管理原則評估

金管會公告金融服務業辦理數位身分驗證指引，應用風險等級與身分驗證機制信賴等級相互適配，研提「證券暨期貨業者線上服務身分驗證實務作業參考」。

線上身分驗證機制信賴等級建議

「證券暨期貨業線上服務」服務項目

業務別

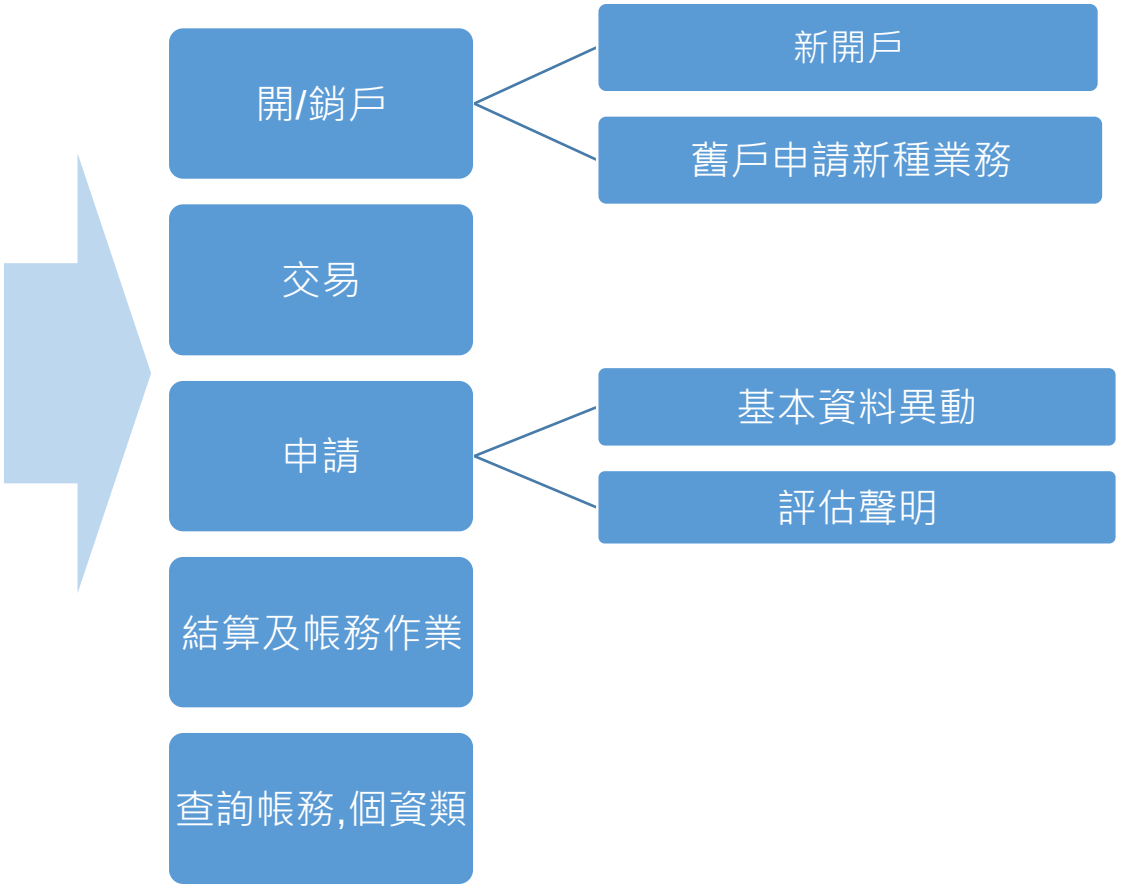
證券 (共106 項)

1. 證券經紀 (含台股、複委託、財管、新金、期貨IB、債票券)
2. 承銷
3. 股代 (集保eCounter)

期貨 (共53 項)

1. 期貨 (含期貨商-經紀、期貨服務事業-顧問/經理/槓桿交易商)

業務類別 (依業務風險及屬性歸類為五大類)



ISO 31000風險矩陣評估業務風險

- 以業務風險原則結果套用及ISO 31000風險矩陣，以強化業務風險原則之方法論。
- ISO 31000風險矩陣中既有之Negligible及Very Unlikely維度，考量採保守態度及難以確保風險極低、微不足道或不會發生，故採4x4風險矩陣圖作為評估。
- 透過ISO/IEC 29115評估決定失效風險(Level of Risk,LoR)，並根據所屬之業務，評估X軸之作業種類風險，決定最終之業務風險。

作業層面影響

申請(評估、聲明等)；查詢

結算及帳務作業；申請(基本資料異動等帳戶、交易直接相關)；開/銷戶 (新種業務申請)

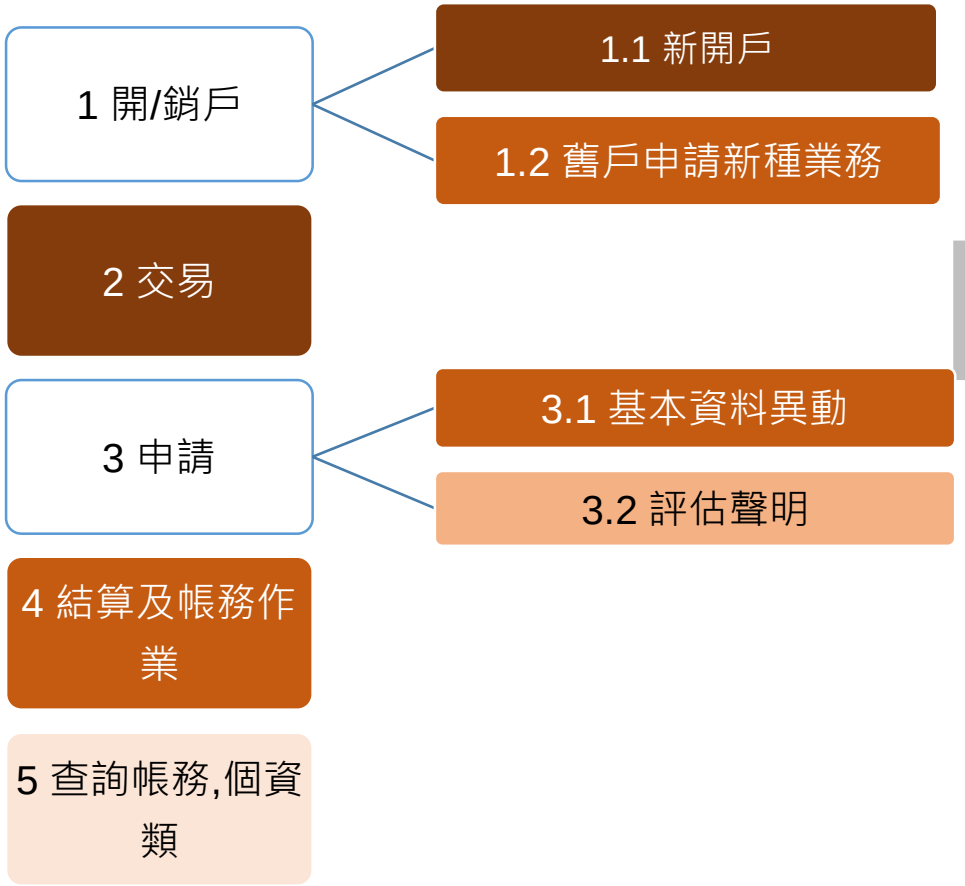
交易；開/銷戶 (新開戶)

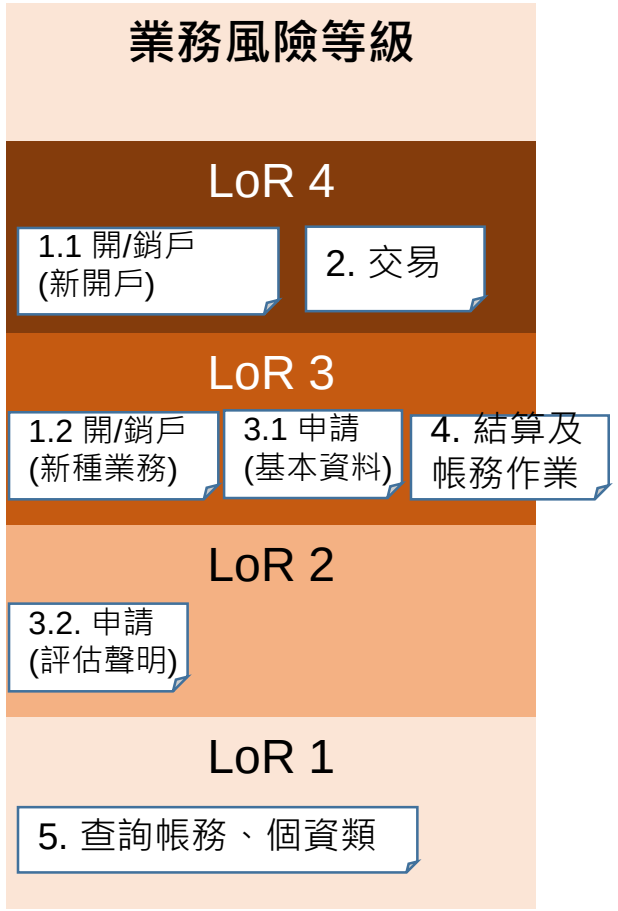
以證券商交易類別為例

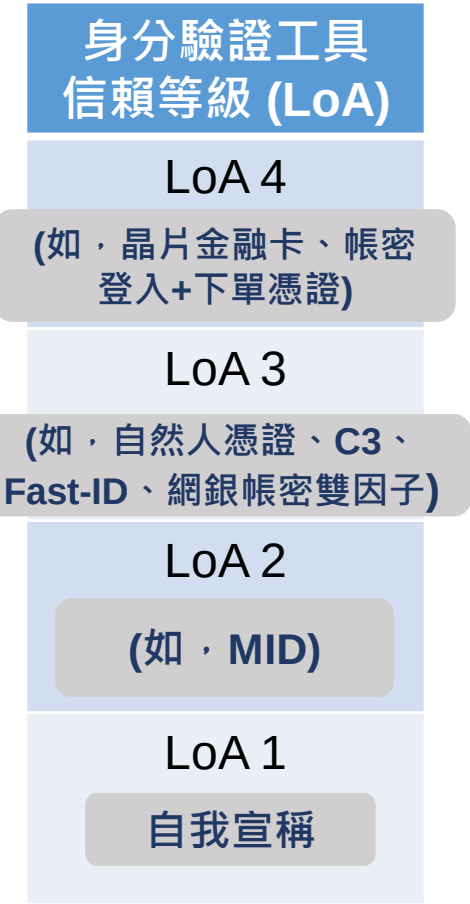
失效風險	Minor	Moderate	Significant	Severe
Very High	LoR 2	LoR 3	LoR 4	LoR 4
High	LoR 1	LoR 2	LoR 3	LoR 4
Medium	LoR 1	LoR 2	LoR 3	LoR 3
Low	LoR 1	LoR 1	LoR 2	LoR 3

金融產業規範參與(1) -
證券暨期貨線上身分驗證實務作業參考 期中成果

證券、期貨159項業務，歸納為5大類







ISO 29115 個體驗證信賴框架及定義

憑證用戶身分識別強度須達保證等級三

電簽法子法「數位簽章憑證實務作業基準應載明事項」(草)

新增 憑證用戶初始身分識別與認證程序 要求

[新增]

第十二條第二項

用戶**初始註冊身分識別與認證**程序之保證等級強度至少應相當於下列標準之一者，始得推定為用戶本人：

(一)**ISO/IEC 29115「高度」(high)以上**等級。

(二)美國 **NIST SP 800-63A** 數位身分指引**「二」(IAL2)以上**等級。

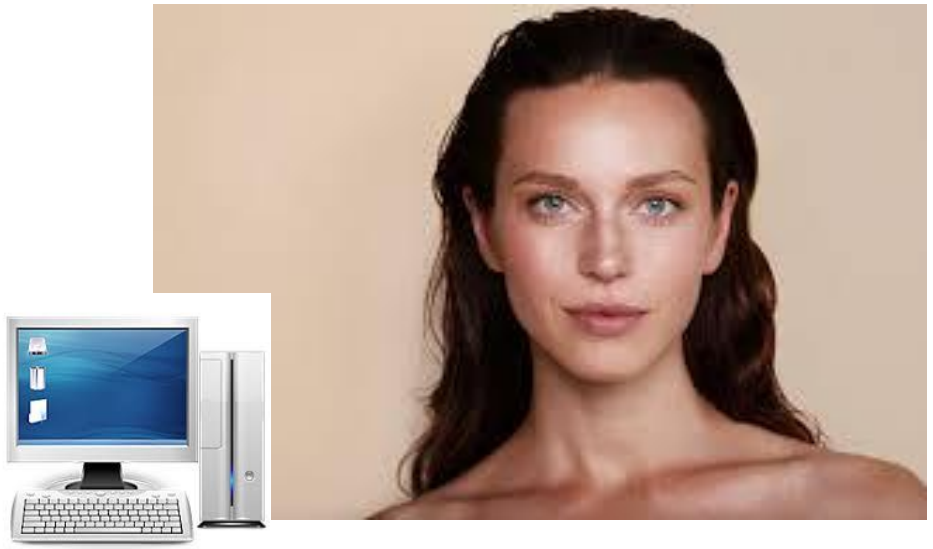
(三)歐盟 **eIDAS** 規則定義之數位身分保證等級**「實質」(Substantial)以上**等級。

ISO/IEC 29115 (enrolment)		NIST IAL (SP 800-63A)		eIDAS	
LoA 1	用戶自我宣稱或證實所提具之身分資訊具唯一性	等級1 (基本)	自我宣稱之身分便具有效力	低信賴	自我聲稱之身分便具有效力。 如，網頁註冊行為。
LoA 2	滿足LOA 1及身分客觀存在：由可靠來源之資料提供方確保資料正確性及有效性	等級2 (高)	需**親自提供證據**進行身分證明	實質 可信賴	**需親自提供身分證明資訊，經確認身分證明資訊後完成身分驗證** 如，輸入帳號密碼後通過OTP驗證。
LoA 3	滿足LOA 2及身分經一個可靠管道驗證：由用戶提示經可靠資料來源核發的**LoA3**信物，並經**信任第三方**驗證	等級3 (極高)	需**臨櫃或在線上經監控下親自提供證據**進行身分證明	高信賴	**需臨櫃或在線上經監控下親自提供證據進行身分證明**。 如，使用自然人憑證卡片。
LoA 4	滿足 LOA 3 及以下要求： • 提示**二個可靠身分 (至少一個達LoA3)**經**信任第三方**驗證 • 自然人須經人工查驗 (witnessed in-person, 如:臨櫃,專人電訪,視訊)				

名詞定義

這裡所謂的「個體」，即為被「驗證身分」的標的。如前一章節所述，個體可以是自然人、法人，甚至也可以是一台伺服器、一個系統或是應用程式。

個體 entity



身分 identity

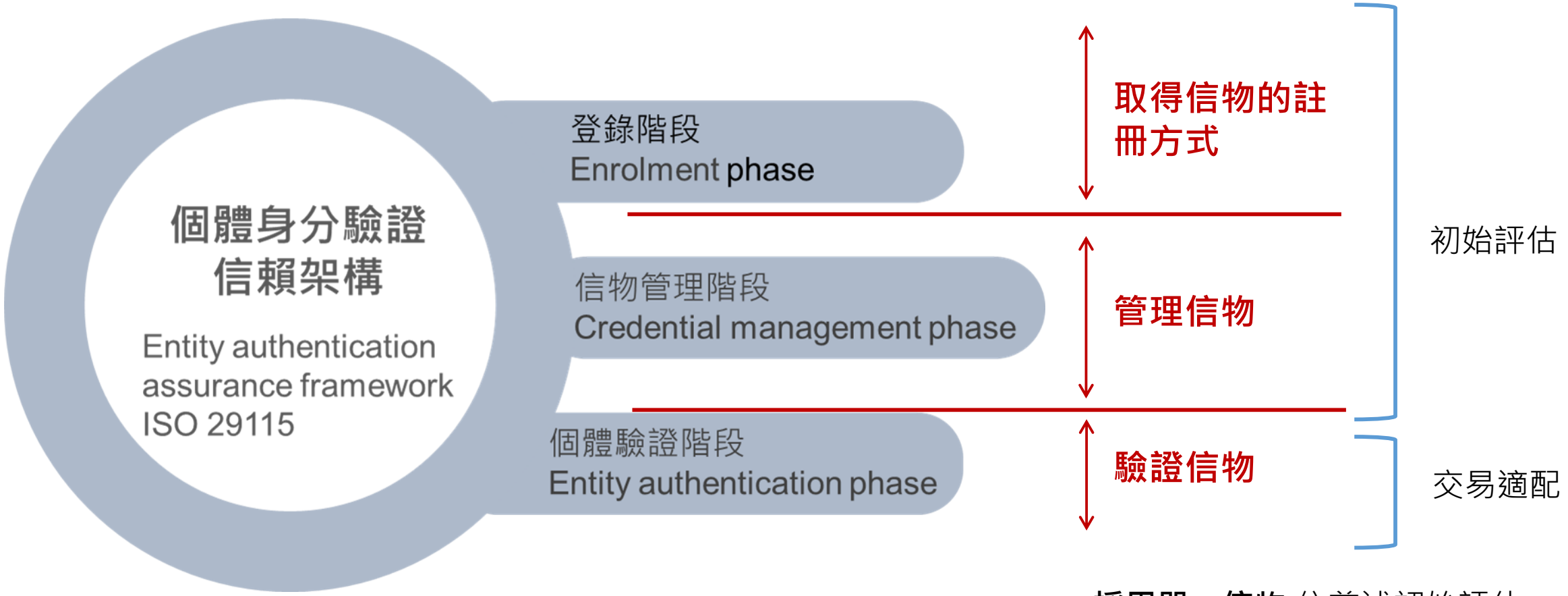
所謂「身分 (identity)」，是由一組關聯於某個「個體 (entity)」的「屬性 (attribute)」所組成的集合 (A set of attributes related to an entity)。

身分驗證 authentication

當一個「個體」宣稱他具備某種「身分」的時候，得以某種既定的機制，驗證該「個體」與「身分」之間的關係，這個驗證的過程稱之為「身分驗證 (authentication)」。

身分 identity

ISO 29115 個體身分驗證信賴架構



- **採用單一信物**:依前述初始評估
- **採用信物組合**:依組合原則重新進行評估

信物 LoA 評估方式

1 單一信物身分驗證機制 LoA 評估

登錄階段
LoA 1
LoA 2
LoA 3
LoA 4

信物管理
LoA 1
LoA 2
LoA 3
LoA 4

身分驗證機制
初始評估

LoA = 2
(取兩個階段較低者)

(現行法規、主管機關已核准或相關函釋另有規定者，從其規定)

2 依業務風險適配身分驗證機制

業務風險	身分驗證機制
LoR 1	LoA 1
LoR 2	LoA 2
LoR 3	LoA 3
LoR 4	LoA 4

若以二個信物組合請參考”信物組合之LoA”

身分登錄階段要求

信賴等級	身分登錄
LoA 1	• 用戶自我宣稱或證實所提具之身分資訊具唯一性(可辨識唯一身分)
LoA 2	滿足 LoA 1 及以下要求： • 身分客觀存在：由可靠來源之資料提供方確保資料正確性及有效性
LoA 3	滿足 LoA 2 及以下要求： • 由用戶提示經可靠資料來源核發的LoA3信物並經信任第三方驗證
LoA 4	滿足 LoA 3 及以下要求： • 提示二個可靠身分 (至少一個達LoA3) 經信任第三方驗證 • 自然人須經人工查驗 (witnessed in-person, 如:臨櫃,專人電訪,視訊等)

- 用戶提供自我宣稱的身分資料
- 用戶提供由可靠來源核發的信物，由信物本身可以客觀認定正確性及有效性
- 提供一個達 LoA 3 的信物
- 身分資料經第三方驗證
- 提供來自兩個可靠管道的身分資料
- 經人工查驗 (臨櫃/類臨櫃)

信物管理階段要求

信賴等級	信物管理
LoA 1	• 信物有制定作業安全政策及作業程序(如:啟用,綁定,保存,更換及撤銷等) • 信物或產製信物方式，須由用戶或業務承辦人員啟用 • 相關數據須保存，並應採取措施以防遭竄改或資訊洩漏 • 應對個資採取保護措施
LoA 2	滿足 LoA 1 及以下要求： • 信物必須加密保護 • 信物必須親自交付或檢查交付方式與該用戶合理關聯
LoA 3	滿足 LoA 2 及以下要求： • 信物啟用時須驗證個體和信物關聯性 • 信物具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態) • 若信物作業程序包含更換/展期，依身分登錄 LoA2 以上進行身分核驗
LoA 4	滿足 LoA 3 及以下要求： • 必須採用防竄改之硬體裝置保存信物，以防被非法匯出或複製 • 若信物作業程序信物包含簽收及保存，須經用戶或其授權代理人同意 • 若信物作業程序包含啟用，只允許在指定時間內完成 • 若信物作業程序包含更換/展期，依身分登錄 LoA3 以上進行身分核驗

信物組合之 LoA 原則 (建議方案)

註:參考 ISO 29115 個體驗證要求

身分驗證組合
(信物組合)

原則 1：兩個風險互補的信物

原則 2：彼此申請時沒有關連性，且兩個信物之間須有共同身分資訊可供勾稽

原則 3 ：兩個信物至少有一個身分登錄滿足欲提升之信賴等級

舉例來說,我們希望信物組合 LoA =3，可以依下列步驟產生。

1. 找到一個身分登錄階段 LoA =3 的機制
2. 找到另一個風險有互補性的信物 (如:雙因子,或同一因子但來自不同申請管道)
3. 檢查這二個信物在申請時是否存在關連性？

當通過這三項檢查後，就可產生一個 LoA =3 的信物組合

(現行法規、主管機關已核准或相關函釋另有規定者，從其規定)

信物組合範例

組合1

	身分登錄 LoA	信物管理 LoA	信物初始評估 LoA
信物 A	2	3	2
信物 B	2	2	2

原則 1：兩個風險互補的信物→ 假設滿足
原則 2：彼此申請時沒有關連性，且兩個信物之間須有共同身分資訊可供勾稽 →假設滿足
原則 3 ：兩個信物至少有一個身分登錄滿足欲提升之信賴等級 → 不滿足,因為想升級至 LoA 3,至少要有一個信物身分登錄達到 LoA 3

組合1 (信物 A + 信物 B) = LoA 2

組合2

	身分登錄 LoA	信物管理 LoA	信物初始評估 LoA
信物 C	3	2	2
信物 B	2	2	2

原則 3 ：兩個信物至少有一個身分登錄滿足欲提升之信賴等級 → 滿足,因為想升級至 LoA 3,至少要有一個信物身分登錄達到 LoA 3

組合2 (信物 C + 信物 B) = LoA 3

結論

電子簽章

典範轉移

身分識別

導入框架

創新服務生態圈

共享共榮