資安防護下的數位身分驗證

臺灣網路認證公司

TWCA 臺灣網路認證

TWID 身分識別中心

大綱

1. 資安事件頻傳
2. 證券客戶身分之資通防護規範
3. 資安防護下的數位身分驗證方案
   - MID KYC
   - MID 企業門號確認
   - 撞庫強化
   - 零信任
   - 網站實名

委外廠商管理不當造成個資外洩

NEWS

微笑單車官網遭受境外 IP 網路攻擊

微笑單車官方網站於2023/5/17遭到駭客網路攻擊，發現有境外IP嘗試取得會員帳號與密碼的情況。

YouBike微笑單車遭駭客侵入，導致2.1萬會員資料恐被竊取，為了彌補會員，微笑單車26日也公布最新補償方案！微笑單車表示，**補償方案為提供相關會員每人500元之YouBike 2.0 騎乘券，目前騎乘券機制已進行開發中，將於112年9月份可上線使用**。

微笑單車 action

- 微笑單車已通報政府相關主管機關及提供資訊予檢調單位進行調查，並同步依照ISO27001及BS 10012個資管理標準，進行全面系統潛在風險盤查，避免再發生。

一. 提升密碼強度，並定期變更密碼；
二. 留意會員帳戶內資料是否正確，以及是否有不明卡片與異常騎乘記錄；
三. 若收到不明的來電、EMAIL或簡訊要求匯款或轉帳，請不要開啟或點擊網址連結；若有欠費，請勿匯款，請至車機、車柱或服務中心辦理繳納。若對資訊有任何疑問，歡迎撥打YouBike客服電話進行確認，本公司客服人員將竭誠為您服務。

資料出處:數位時代,https://www.bnext.com.tw/article/75330/youbike-cyber-security ,2023/6/30擷取

單一企業個資事故恐造成連鎖效應

NEWS

電子發票平台資安爆漏洞 逾 7% 上市櫃公司營業隱私恐外洩

READr 近日接獲民眾提供一份包含 130 家上市櫃公司的名單，指稱財政部負責的「電子發票整合服務平台」登入系統出現資安缺失：只要輸入名單上企業的統編，以及政府提供的預設密碼，即可瀏覽其會員資料。也就是說，**只需使用同一組密碼，包括發票明細、營業收入等企業經營之重大商業資料將一覽無遺**。

根據此份名單，1789 間上市上櫃公司中就有超過 7% 的企業仍沿用政府提供的預設密碼，其中 78 間為上市公司、52 間為上櫃公司。從產業別來看，光電業最多，其次是半導體業、電子零組件業，甚至連專門從事資訊安全的公司也榜上有名...。

資料來源：鏡周刊，
https://www.mirrormedia.mg/story/20230516readr001/ (2023.5)

財政部 action

- 整合服務平台營利事業密碼弱點已改善完成
- 推動新版「**雙認證模式**」。以舊預設密碼登入後即強制變更密碼，並應輸入第二因子，始得使用整合服務平台服務

《take away》

1. 資安、個資保護政策，需要落實於產品、服務流程
2. 客戶完成Onboarding後，後續登入應留意身分驗證機制具備可信賴度
3. 最後，安全風險無法一勞永逸，新興科技、犯罪手法衍生之風險議題，應定期、不定期分析及因應

電商網站個資頻傳

蝦皮購物　誠品書店 elite bookstore

NEWS

蝦皮,誠品個資外洩未改善遭罰款

蝦皮、誠品生活及旋轉拍賣等業者涉及消

蝦皮對委外廠商未落實稽核，未能提供完整的安全管控執行、稽核紀錄等具體佐證資料，無法證實該公司對保有個資已採行適當之安全措施，因此依據《個資法》第48條第4款併第50條規定，處分業者併同其負責人罰鍰計新臺幣20萬元。

誠品生活案，經數位部產業署實地行政檢查，現場已發現在帳號管理上執行未確實，另要求事後提供之補充或佐證資料，該公司個資盤點資料仍不完整，且針對委外廠商監督管理未落實執行，因此依據個資法第48條第4款併第50條規定處分，業者併同其負責人罰鍰計新臺幣10萬元。

數位發展部

已要求前述業者落實個資法相關規定，並限期請業者再為改正，如屆期未改正，將按次處分。同時數位部要求各電商業者務必重視個資保護，並且數位部也會引入相關解決方案例如隱碼技術，與電商業者合作，持續強化個資保護措施。

資料出處:數位時代，https://www.bnext.com.tw/article/74423/shopee-data-breach, 2023/6/30 擷取

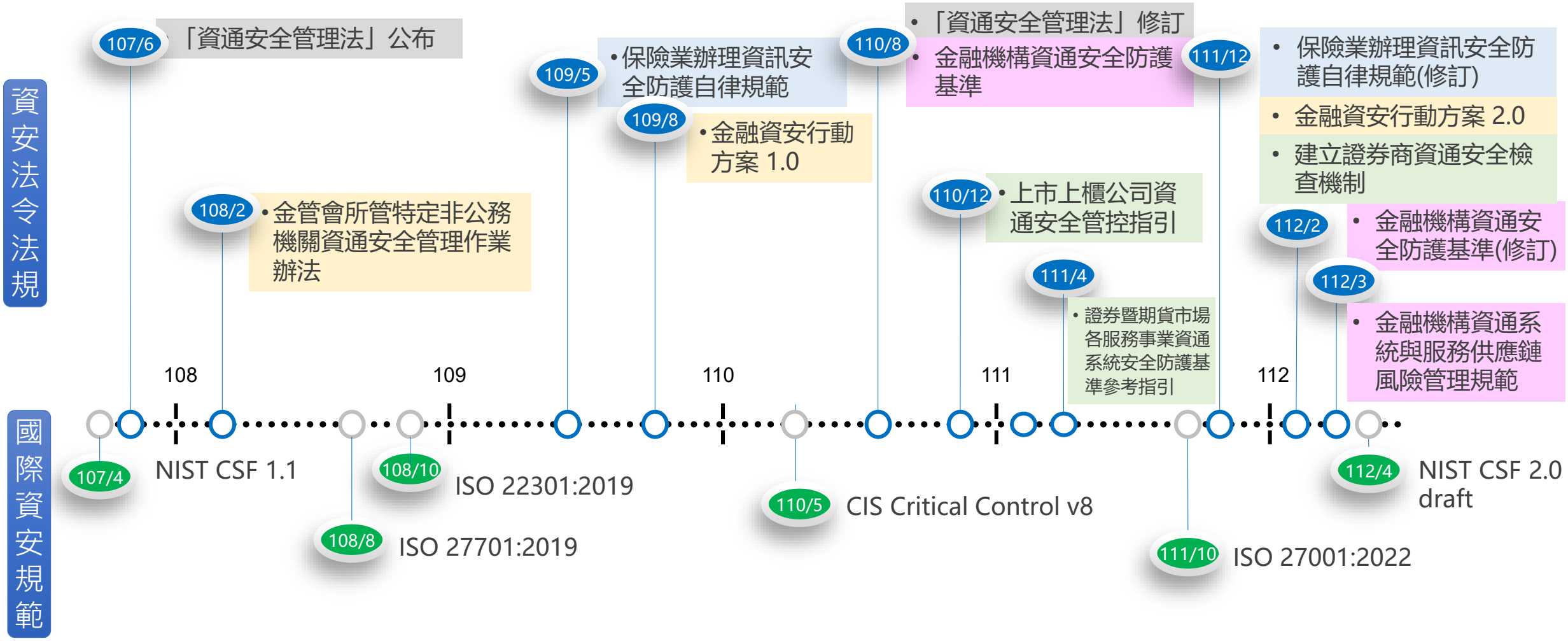
近期資通安全事件解析 - 1

新聞事例	資通安全 風險	資通安全要求 關鍵議題	企業管控措施 可強化方向
微笑單車公司 「YouBike」	「YouBike」系統遭境外及境內網路攻擊，致約有4萬多名會員交易的資料，包含手機號碼、密碼、卡號及交易資料可能遭竊取	委外	第29條 1. 訂定資訊作業委外安全管理程序，包含委外選商、監督管理(如：對供應商與合作夥伴進行稽核)及委外關係終止之相關規定，確保委外廠商執行委外作業時，具備完善之資通安全管理措施。 第30條 1. 訂定委外廠商之資通安全責任及保密規定，於採購文件中載明服務水準協議(SLA)、資安要求及對委外廠商資安稽核權
		開發安全	第13條 1. 將資安要求納入資通系統開發及維護需求規格，包含機敏資料存取控制、用戶登入身分驗證及用戶輸入輸出之檢查過濾等。 第16條 1. 對核心資通系統辦理下列資安檢測作業，並完成系統弱點修補。 a.定期辦理弱點掃描。 b.定期辦理滲透測試。 c.系統上線前執行源碼掃描安全檢測。
財政部 發票平台	財政部發票平台爆資安漏洞，只要輸入企業統編、政府提供之預設密碼，就可以瀏覽器超過130家上市櫃公司資料，甚至包含國營事業及國安單位的採購資訊	存取控制、身分驗證管理	第21條 1. 建立使用者通行碼管理之作業規定，如：預設密碼、密碼長度、密碼複雜度、密碼歷程記錄、密碼最短及最長之效期限制、登入失敗鎖定機制，並評估於核心資通系統採取多重認證技術。

近期資通安全事件解析 - 2

新聞事例	資通安全風險	資通安全要求關鍵議題	企業管控措施可強化方向
蝦皮、誠品生活	蝦皮、誠品生活未依照個資法採取適當資安措施，遭數位部開鍘各罰20萬、10萬	個資盤點、風險評估	第11條 1. 定期盤點資通系統，並建立核心系統資訊資產清冊，以鑑別其資訊資產價值。 第12條 1. 定期辦理資安風險評估，就核心業務及核心資通系統鑑別其可能遭遇之資安風險，分析其喪失機密性、完整性及可用性之衝擊，並執行對應之資通安全管理面或技術面控制措施等
		資通安全防護及控制及監控	第18條 1. 具備下列資安防護控制措施： a. 防毒軟體。 b. 網路防火牆。 c. 如有郵件伺服器者，具備電子郵件過濾機制。 d. 入侵偵測及防禦機制。 e. 如有對外服務之核心資通系統者，具備應用程式防火牆。 f. 進階持續性威脅攻擊防禦措施。 g. 資通安全威脅偵測管理機制(SOC) 第19條 1. 針對機敏性資料之處理及儲存建立適當之防護措施，如：實體隔離、專用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽、人員管理及處理規範等。 2. 建立資通系統及相關設備適當之監控措施，如：身分驗證失敗、存取資源失敗重要行為、重要資料異動、功能錯誤及管理者行為等，並針對日誌建立適當之保護機制。

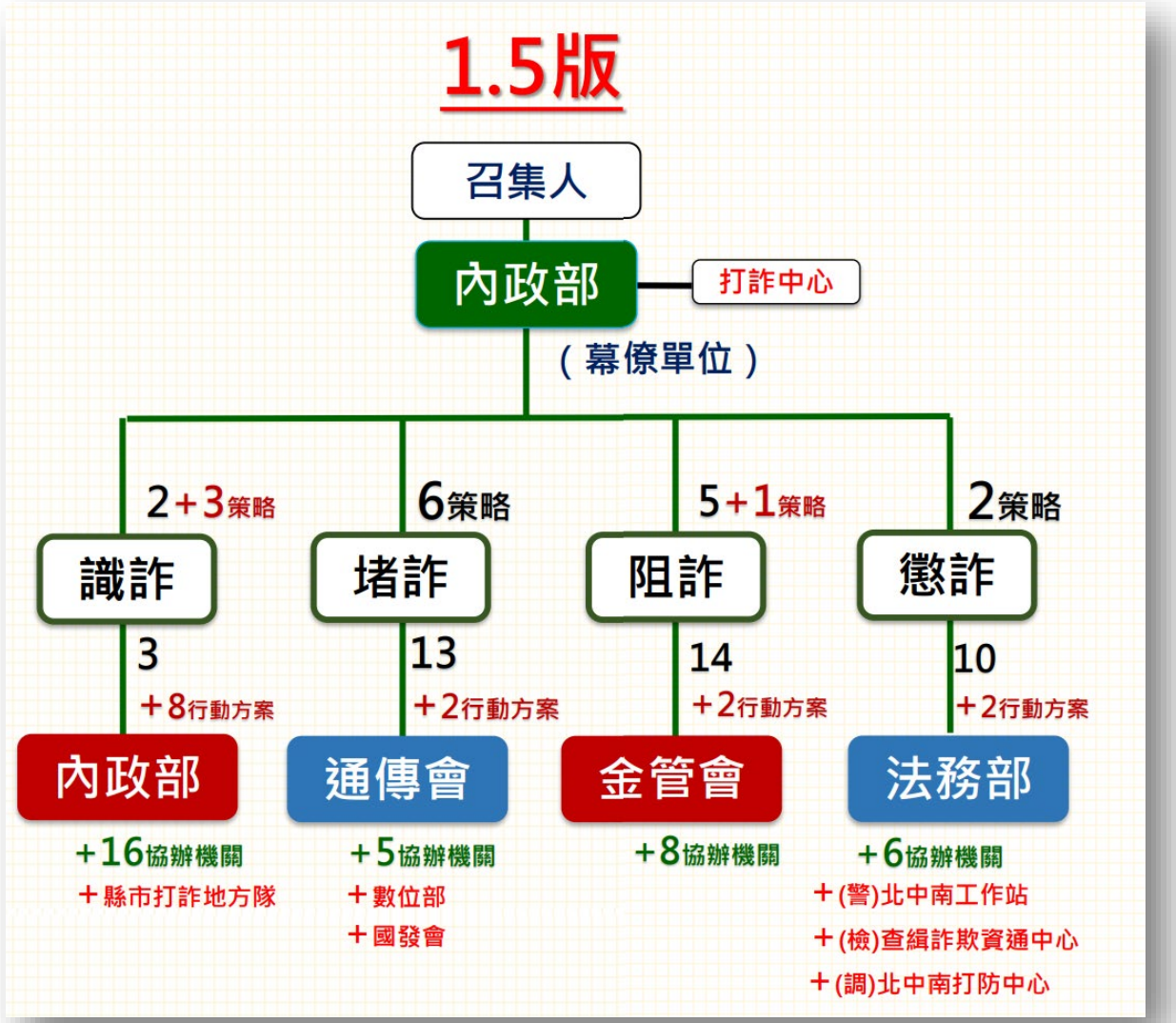
金融資通安全環境逐步成熟



資通科技發展導致詐欺樣貌多樣化

資通科技詐欺用途	特性	常見詐騙手法	詐術施行技術含量	共通點
詐欺工具	針對特定受害人，利用資通工具使本人違反其意願為匯款等行為。	如，社交工程、勒索病毒	高	客戶資料(直接/間接個資、或營業等資料)外洩，為詐欺集團用於不法用途。
詐欺場所	面對不特定一般人，以名人冒名、假網站等詐術使人交付本人或第三人財產。	如，假投資、一頁式詐騙	低	
詐欺客體	針對目標系統或網路進行惡意攻擊，以影響目標對象服務可用性。	如，網頁替換	中	

政府四路打詐，以增加 詐欺成本 為行動目標



- 2022年7月15日行政院訂頒「新世代打擊詐欺策略行動綱領」，由內政部主責

- 2023年5月14日政院推「打詐1.5版」
  - 強化申請約定轉帳防詐
  - 納管虛擬資產交易平台業者
  - 就源處理網路假投資廣告
  - 遊戲點數防詐鎖卡及內控機制
  - 第三方支付業者建立客戶審查機制
  - 全台走透透宣導防詐

詐騙路徑及手法

詐騙集團　　中介管道　　民眾

人頭 / 車手 —開戶 (洗錢人頭帳戶)→ **銀行**

月租型人頭門號
企業門號
預付卡門號 —代收簡訊認證碼、申請免洗帳號→ **社群平台**

透過社群購買商品，付錢但拿不到貨
賣家可隨時砍帳號
受騙買家 → **社群平台**

詐騙網頁 —不實廣告上架→ **廣告平台**

民眾 —導向詐騙網頁、騙取個資/金錢→ **廣告平台**

詐騙集團 / 偽造網頁 —發送惡意簡訊→ **簡訊業者**

TA: 金融機構 → **簡訊業者**

證券客戶身分之資通防護規範

證券商客戶身分防護法遵要求

依據	規範內容	法遵重點
上市上櫃公司資通安全管控指引(111.4.7)	第五章 資通系統發展及維護安全 第13條、將資安要求納入**資通系統開發及維護需求規格，包含**機敏資料存取控制、**用戶登入身分驗證**及用戶輸入輸出之檢查過濾等。 (*See* also 第14條 定期測試、第23條 監控措施)	資安精神應落實於資通系統開發及維護。其中資安要求包含**身分驗證機制**
建立證券商資通安全檢查機制(111.12.28)	第7點 通訊與作業管理(CC-17000) d. CA認證與憑證管理 (a) 網路下單證券商應訂定憑證交付程序，避免非本人取得憑證。客戶申請或更新憑證下載，**必須採用多因子（如：下單憑證、綁定裝置、OTP、生物辨識及SIM認證等）驗證方式，且與登入帳戶時使用之因子不同，確實辨認客戶身分**並留存紀錄。	憑證管理之多因子驗證應與客戶登入時使用之因子有別，以確保**身分驗證機制有效**
證券商受理線上開戶委託人身分認證及額度分級管理標準 (111.12.16)	證券商就線上開戶程序，應於內部控制制度自行訂定相關作業流程。**受理該類開戶作業除應確定其身分為本人及留存相關證明文件外，應先經下列第三方認證或出具本人證件以確認身分**： 一. 經往來交割銀行確認。 二. 經線上傳送自然人憑證、銀行帳戶或晶片金融卡等。 三. 經線上傳送可同時辨識國民身分證及臉部之照片，並輔以證券商交割專戶客戶分戶帳指定出金帳戶。 四. 經由視訊影像方式確認。 五. 經由行動身分識別（Mobile ID）方式確認，相關身分認證應遵循事項由本公司另訂之。 六. 透過其他可確認身分之方式 。	身分驗證機制之可信賴性，應透過**第三方認證**

ISO 29115標準之身分識別機制

階段	簡稱	主要作業內容
登錄階段 enrolment phase	登錄 enrolment	核驗並確認個體所提示的身分資料與個體之關聯性。 將完成核驗「實體世界的個體」所對應的「身分資料」進行登錄作業。
信物管理階段 credential management phases	管理 management	建立並維護個體與身分資料的關聯性。 除了管理「信物」產製、發放以及維運的整個生命週期外，尚須維護身分資料與信物之間的「連結性」及資料的「正確性」與「即時性」。
個體驗證階段 entity authentication phase	驗證 authentication	驗證個體與身分資料的關聯性。 個體提出服務相對應所需之信物，而藉由驗證信物獲得個體身分資料的過程，即為「驗證」。

信賴等級 (LoA)	說明 (對所驗證之身分的可信度)
LoA1	(Little or no) 少許或沒有可信度可言
LoA2	(Some) 具某種程度的可信度
LoA3	(High) 高可信度
LoA4	(Very high) 極高可信度

身分認證及額度分級管理標準

法規:臺灣證券交易所股份有限公司證券商受理線上開戶委託人身分認證及額度分級管理標準(111年12月16日公佈)

帳戶類型	身分認證程序	約定強度	單日買賣最高額度
第一類	一. 往來交割銀行確認。 二. 自然人憑證、銀行帳戶或晶片金融卡等資料。 三. 可同時辨識國民身分證及臉部之照片+證券商交割專戶客戶分戶帳指定出金帳戶。 四. 視訊影像方式確認。 五. 行動身分識別（Mobile ID）方式確認。 六. 其他可確認委託人方式。 **以上都需結合 OTP 或電訪。**	同意單日買賣最高額度受限。	新臺幣100萬元。
第二類	自然人憑證+視訊影像方式。	提供資力證明，如個人年所得扣繳憑單資料等。	依徵信與額度管理自律規則，由證券商自行訂定評估單日買賣最高額度。
第三類	同第一類。	約定於委託買賣時採預收或圈存方式辦理。	比照第二類辦理。

證券商行動身分識別(Mobile ID)身分認證

證券商辦理行動身分識別(Mobile ID)身分認證應循事項 (111.12.16)

第二條
行動身分識別（Mobile ID），係指證券商經取得委託人同意後，由委託人透過載有4G以上門號SIM卡之行動裝置，經第三方認證機構向委託人所屬之電信業者，以委託人之行動電話號碼、國民身分證統一編號及生日，與電信業者之行動門號租用人申辦資料進行比對，確認為一致後通知證券商，所進行之身分認證作業。

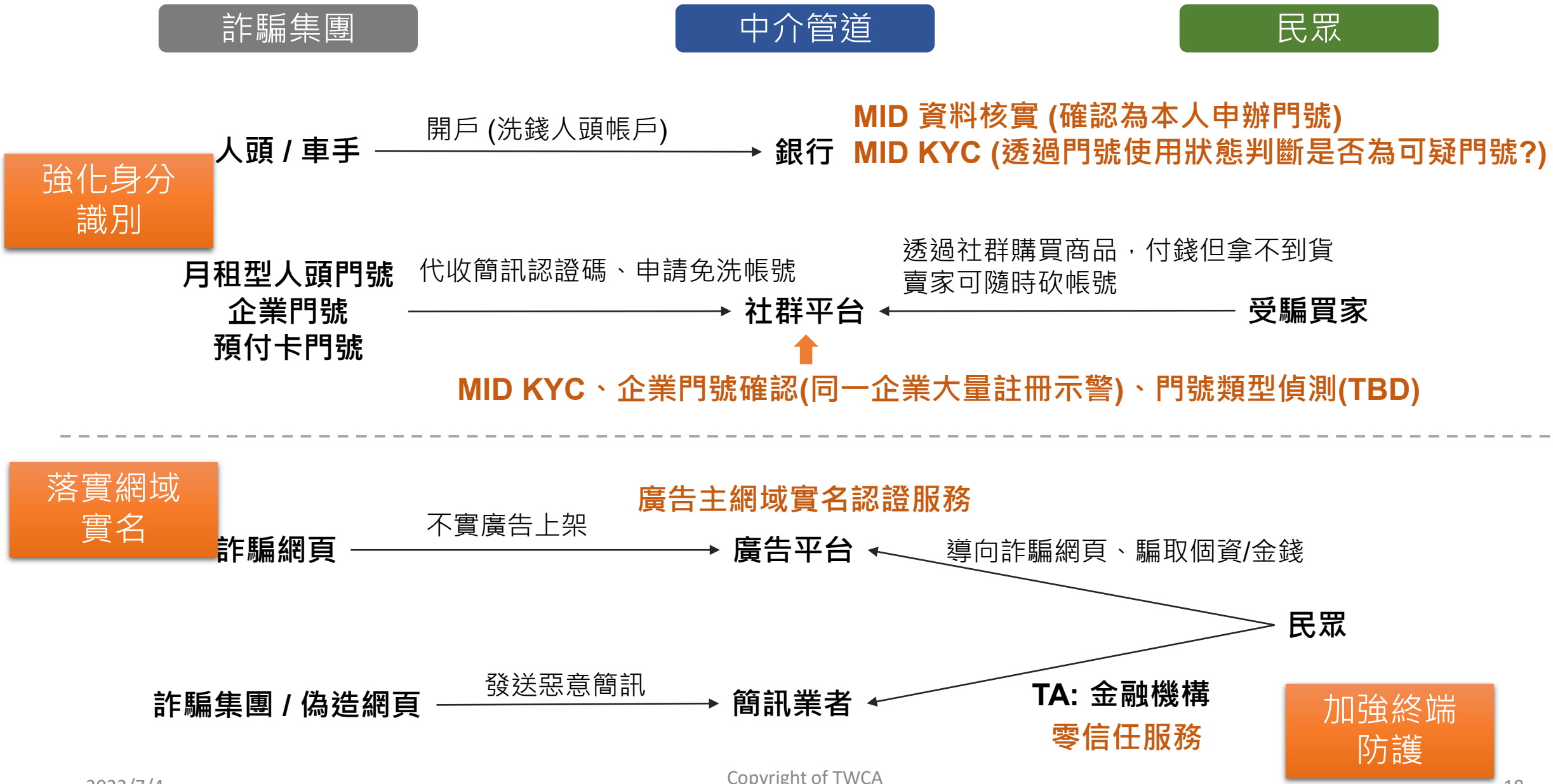
前項所稱4G以上門號，係指委託人至電信業者直營門市臨櫃申辦，交付國民身分證及具辨識力之第二身分證明文件並完成親簽後申辦之門號，且應排除儲值卡、親子卡、預付卡、企業卡、委託代辦等無法辨識本人親辦親簽之門號。

本事項所稱第三方認證機構，係指數位發展部依電子簽章法第十一條第四項規定公告核定之憑證機構。

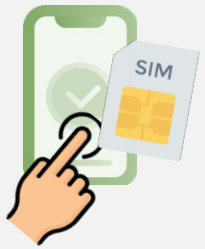
資安防護下的數位身分驗證方案

- MID KYC
- MID 企業門號確認

詐騙路徑及手法



行動身分識別 (Mobile ID)



持電信 SIM 卡客戶

TWID 身分識別中心

電信業者

門號身分識別

由電信業者比對門號申辦人留存門號、身分證字號，並確認發動交易的SIM卡與門號相符。

‘識別使用者身分’

SIM 認證

確認目前發動交易的SIM卡和要認證的門號是否相符。

‘驗證約定往來門號’

門號資料核實

由服務提供者發動查詢，門號及申辦人身分證字號是否相符。

‘核實留存資料’

MID 服務於金融產業應用現況

	門號身分識別	SIM 認證	門號資料核實
	‘識別使用者身分’	*‘驗證約定往來門號’*	*‘核實留存資料’*
銀行	**跨境支付會員帳號註冊**	**客戶設備綁定** **重新設定交易密碼** (22 家銀行)	**客戶門號定期核實**
保險	**網路會員帳號註冊** **遠距投保** **行動投保** (10 家業者)	推廣中	**保戶門號定期核實**
證券	**變更原留手機門號**	推廣中	推廣中
政府	**線上服務實名認證** (防疫、報稅、報關、勞保)	推廣中	**MyData 會員手機核實**

New

MID 企業門號確認

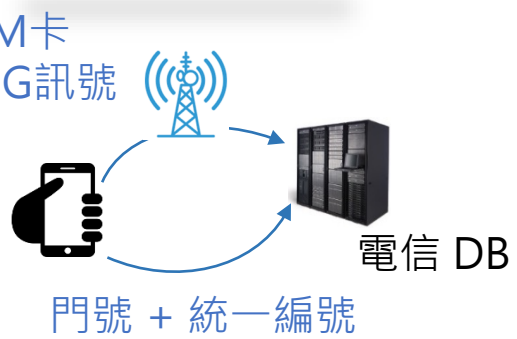
- 提供**統一編號 + 門號**作為識別因子，由電信業者判斷是否為既有的企業用戶。
- 僅能確認該門號為企業申辦，如需識別自然人，建議搭配其他檢核因子。

應用場域

身分識別機制
之**輔助因子**

驗證是否為
企業申辦之門號

企業門號確認



企業門號資料核實

發動者	用戶手機端	SP 主機端
可驗資料	1. SIM 卡 2. 門號 3. 統一編號	1. 門號 2. 統一編號
驗證限制	需使用4G/5G網路連線	無

New

MID KYC

門號樣態確認

手機(SIM卡)發動：身分證字號(ID) + 門號

TWID 身分識別中心

1. 該門號為該 ID 申辦
2. 該 ID 持有該門號是否**超過 6 個月**(門號換號或過戶..不在此限)
3. 該門號電信費帳單繳費方式是否為**自動繳款**(限金融帳戶及信用卡)
4. 該門號近6個月是否曾進入**催繳狀態**(催繳狀態僅限該門號或與該門號合併之帳單)

姓名確認

手機(SIM卡)發動：身分證字號(ID) + 門號 + 姓名(王大明)

TWID 身分識別中心

1. 該門號為該 ID 申辦
2. 該門號登記姓名是否為王大明

* 限制及資格同 MID 門號身分識別

電信使用樣態

租約期間紀錄

中華電信 Chunghwa Telecom
T STAR 台灣之星
亞太電信 Gt
台灣大哥大
遠傳 FET

MID KYC

申辦銀行業務
線上開戶、
貸放款...等

客戶同意條款

身分識別
樣態檢核

TWID
身分識別中心

客戶身分識別及電信使用樣態檢核結果

服務整合優勢

- 用戶實名認證
- 評估信賴程度
- 打擊詐欺行動

發現潛在問題點

攔阻詐騙可能性

預防人頭或車手

強化檢核因子

- 持有門號是否超過6個月
- 是否綁定金融繳款工具
- 近 6 個月是否正常繳費

資安防護下的數位身分驗證方案

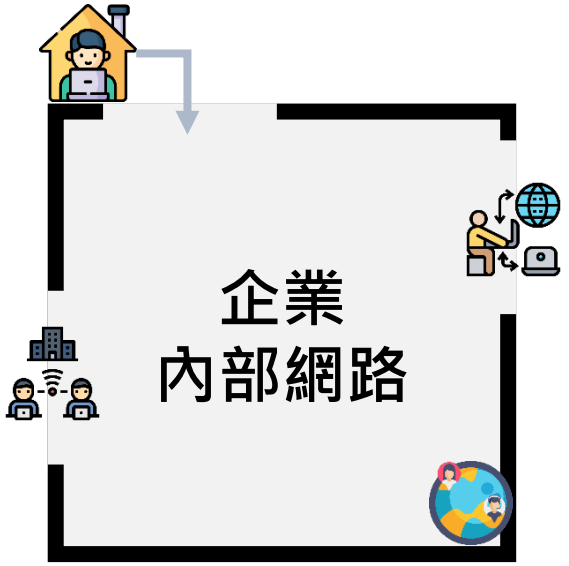
- 撞庫強化
- 零信任
- 網站實名

撞庫事件後的資安強化措施

- 第一是證券商及期貨商應使用優質密碼設定並進行管控
  - 例如：確實執行密碼輸入錯誤次數達3次，必須予中斷連線，及加強宣導客戶定期更新使用者密碼。
- 第二是證券商及期貨商應於網路下單登入時落實採多因子認證方式，
  - 例如：下單憑證、綁定裝置、OTP、生物辨識等機制，強化憑證換發的驗證機制，以確保為客戶本人登入。
- 第三是證券商及期貨商應每日針對核心系統的帳號登入失敗紀錄進行監控
  - 例如：非客戶帳號登入嘗試紀錄等，進行監控及瞭解分析異常登入原因、異常IP登入時通知投資人，並留存相關紀錄。

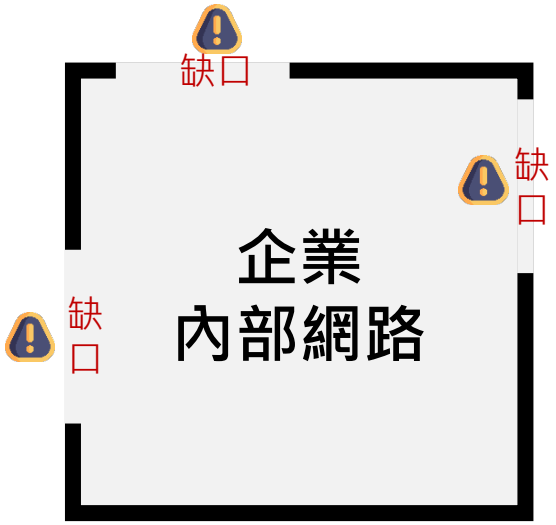
隨著時代發展，網路信任邊界模糊化

工作型態多元化



遠端工作、外包工程、
雲端服務、多元裝置...

信任邊界模糊



疫情製造了更多資安缺口

駭客入侵機會提升

時代演進，駭客能力↑

零信任是什麼?

ZTA (Zero Trust Architecture)

- 是一種資安防護的新概念，打破了傳統以邊界（例如防火牆）區分內網及外網的資安型態
- 一個關於作業流程/系統設計/營運策略的概念及指導原則

ZTN (Zero Trust Network)

- 解決現今網路環境複雜造成信任邊界不明之資安窘境，期望透過對任何資料存取皆永不信任且必須驗證的原則，達成不論在何時何地存取資料皆保證一致安全性之相關技術。
- 參考 NIST (SP 800-207)零信任架構，設計符合國內資安政策之政府零信任網路，採存取門戶部署方式，具備**身分鑑別**、**設備鑑別**及**信任推斷** 3 大核心機制

我不信任您，請您每一次進行服務登入/ 資料存取都要驗證哦！

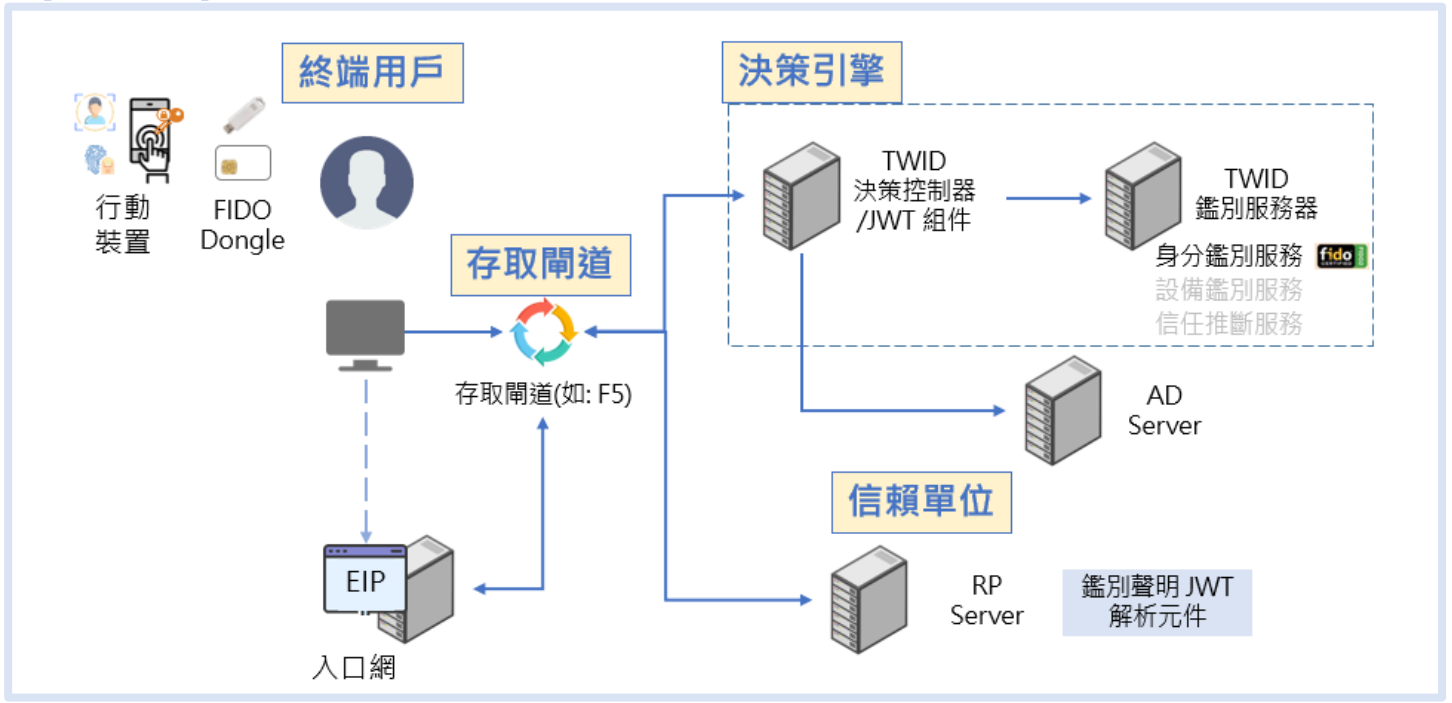
零信任網路 (ZTN) 規劃與原則

導入零信任網路**會是一段過程**，而不是一次大規模替換基礎架構，相關組件之部署須具備能與**現有系統同時混合運作**之能力。

取自：政府零信任網路說明_V1.9_1110712.pdf
https://www.nics.nat.gov.tw/ZeroTrustMain?lang=zh

建議先找單一應用場域導入

零信任網路 (ZTN) 是甚麼?



終端用戶	存取閘道(Access Gateway)	決策引擎(Decision Engine)	機關資通系統/信賴單位(RP)
欲登入 RP 人員	負責網路導向與連線，為 RP之存取門戶 • 不論來自內部或外部網路之存取，**必須且唯一**經由存取閘道 • 為唯一公開存取之組件，存取全程必須隱藏內部網路路徑(如利用**反向代理**技術) • 實施**負載平衡**機制以避免效率瓶頸 • 實施可有效防止阻斷服務攻擊之機制	**A. 決策控制器** B. 三大核心機制 **1. 身分鑑別(111)** 2. 設備鑑別(112) 3. 信任推斷(113) **C. 鑑別聲明伺服器**	• 內部系統 ✓ 公文系統 ✓ 報表系統 ✓ EIP 系統 ✓ 網管系統 ✓ 防火牆系統 • 對外服務

建議先找單一應用場域導入

零信任網路 (ZTN) 三階段規劃

	身分鑑別 (111)	設備鑑別 (112)	信任推斷 (113)
現況	• 仰賴密碼(Password)或 有風險的 MFA	• 首次設定決定未來權限 或未定義	• 首次設定決定未來權限 或未定義
政府走向	• **國際 FIDO 規範** • **私鑰存於 Client端** • **允許生物特徵結合 FIDO Key 簡便密碼輸入**	• **TPM 鑑別**設備安全性 • **動態分析**設備健康信任等級 • **控管設備**存取權限	• 透過**身分鑑別、設備鑑別**及**匯整各類輸入資料**(如:使用者IP) 推估信任分數

零信任網路 (ZTN) 第一階段說明

身分鑑別 (111)

傳統
(現在)

- 仰賴密碼(Passwor
或 有風險的 MFA

政府
走向

- **國際 FIDO 規範**
- **私鑰存於 Client端**
- **允許生物特徵結合 FIDO Key 簡便密碼輸入**

您的指紋有誤！
請重新辨識！

Fast IDentity Online (FIDO)

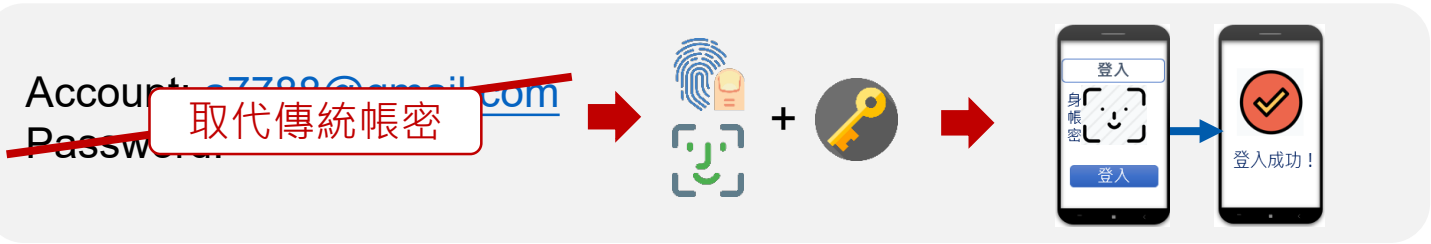
結合**公開金鑰、生物特徵**等技術，提供便利且安全的網路**身分驗證機制**，並依此建立產業標準。

無密碼 解決傳統密碼及 OTP 的安全性不足等問題

國際標準 FIDO 身分識別國際標準

行動化 人手一機，導入快速/體驗最好

安全性 非對稱金鑰之簽驗章技術為基礎



零信任網路 (ZTN) 第一階段說明

身分鑑別 (111)

傳統
(現在)

- 仰賴密碼(Passwor
  或 有風險的 MFA

政府
走向

- **國際 FIDO 規範**
- **私鑰存於 Client端**
- **允許生物特徵結合 FIDO Key 簡便密碼輸入**

您的指紋有誤！
請重新辨識！

臺網 FIDO ID 特色

FIDO Key 結合 憑證 應用更多元

- **系統登入 (身分識別)**
- **強化機制 (多因子機制)**
- **服務申辦 / 主管放行**
- **文件簽署 (不可否認性)**

零信任網路 (ZTN) 第二階段說明

設備鑑別 (112)

傳統
(現在)

- 首次設定決定未來權限
未定義

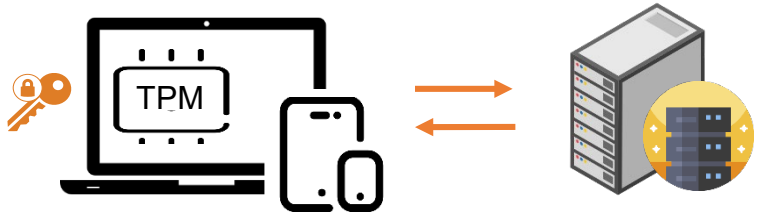
政府
走向

- **TPM 鑑別**設備安全性
- **動態分析**設備健康信任
- **控管設備**存取權限

每次針對設備行安全性檢查
例如設備太舊，可能會顯示
無法滿足資料取用資格！

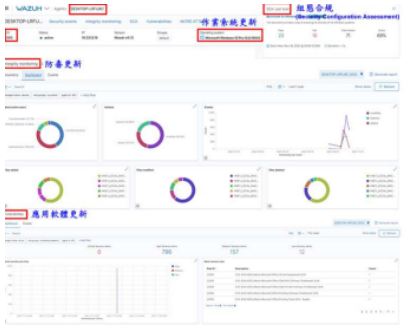
設備 TPM 鑑別

– 執行基於TPM內私鑰之公開金鑰密碼系統鑑別協議



設備健康管理

– 持續更新設備健康狀態
– 依設備健康狀態隨時換算設備健康信任等級



設備編號	設備健康狀態	信任等級
D001	AD	0.5
D002	CD	0.3
D003	ABC	0.9
D004	D	0.1

健康狀態/等級分配
(A)作業系統更新：0.4
(B)防毒更新　　：0.3
(C)應用軟體更新：0.2
(D)組態合規　　：0.1

零信任網路 (ZTN) 第三階段說明

信任推斷 (113)

傳統
(現在)

- 首次設定決定未來權限
  未定義

政府
走向

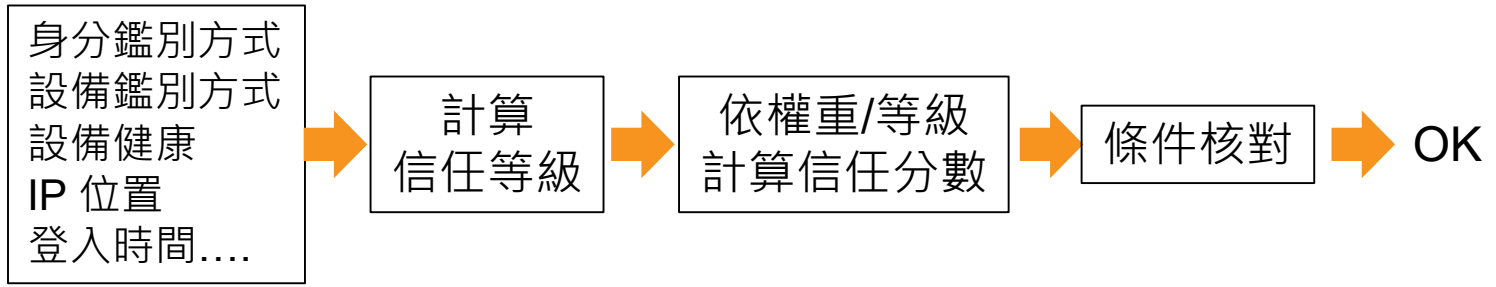
- 透過**身分鑑別、設備鑑**
  匯整各類輸入資料(如
  者IP) 推估信任分數

如果信任推斷的資訊顯示
安全，可能會限制權限或
求重新登入！

信任推斷機制

建置信任推斷前端系統，匯整各類輸入資料，透過信任推斷伺服器，進行(智慧)評估與計算，輸出信任分數

- 輸入：身分鑑別方式、設備鑑別方式、設備健康信任等級、及使用者情境(IP位址、登入時間、瀏覽器等)
- 輸出：信任分數，供決策控制器做存取決策



網站實名制

網站擁有SSL憑證並無法保障網站安全。網路釣魚詐騙中，詐騙集團慣以免費、自動化、開放憑證架設釣魚網站，透過平台投放不實廣告；或利用簡訊夾帶惡意連結，混淆一般消費者或投資者誤信，致個人資料遭洩漏或財產等損失。而企業型憑證或稱延伸驗證憑證（EV SSL/TLS）為具有最高層級加密、驗證和信任之數位憑證。申請EV SSL/TLS時，企業或網站擁有者必須接受憑證機構嚴格審查，審查範圍例如實體公司、使用網域專屬權利等。以驗證等級而言，憑證可區分為以下三類：

項目	基本型（DV）	進階型（OV）	企業型（EV）
驗證等級	域名驗證 (Domain Validation, DV)	組織驗證 (Organization Validation, OV)	延伸驗證 (Extension Validation, EV)
驗證方式	網頁驗證檔、DNS、E-mail	人工驗證	
驗證對象	域名持有人	域名持有人、公司證明文件	域名持有人、公司證明文件、第三方驗證
適用範圍	個人網站	一般商業機構	金融機構、資安防護需求企業
憑證特性	發證快速	憑證登載組織資訊	憑證登載組織資訊、網址列標示組織名稱

敬請指教

臺灣網路認證公司

TWCA 臺灣網路認證

TWID 身分識別中心