FATF

數位身分指引

2020 年 3 月

數位身分指引

2020 年 3 月

防制洗錢金融行動工作組織

FATF（防制洗錢金融行動工作組織）是一個獨立的政府間組織，旨在發展與提升政策，保護全球性金融體系，以對抗洗錢、資恐以及資助絕大規模毀滅性武器擴散。FATF 建議已公認為全球性洗錢防制（AML）與打擊資恐（CFT）的標準。

如欲進一步瞭解 FATF，請參閱：www.fatf-gafi.org

本文件及 / 或本文所含的任何地域，概不影響任何領土的狀態或主權、國際疆界之界定，或任何領土、城市或地區之名稱。

引用文獻：

FATF (2020 年)，《數位身分指引》，FATF，巴黎，www.fatf-gafi.org/publications/documents / digital- identity-guidance.html

本出版品業經 FATF 秘書處授權，由中華臺北行政院洗錢防制辦公室譯為中文，如有出入以公布於 FATF 官網 :www.fatf-gafi.org 之英文版為準。
行政院洗錢防制辦公室 2021 年 12 月印製

目　錄

縮寫對照表

AAL1/2/3	驗證保證等級（依 NIST 規定）
AL	保證等級
AML/CFT	防制洗錢/打擊資恐（Anti-money laundering/Countering the financing ofterrorism）
API	應用程式介面
ASP	驗證服務提供者
CDD	客戶盡職審查
CEN	歐洲標準委員會
CENELEC	歐洲電工標準化委員會
CSP	憑證服務提供者
DCS	文件檢查服務
DLT	分散式分類帳技術
DNFBP	指定之非金融事業或人員
ETSI	歐洲電信標準協會
eIDAS	歐盟第 910/2014 號規章「電子交易在內部市場的電子身分識別驗證和信託服務規則」。
FAL1/2/3	聯合識別保證等級（依 NIST 規定）
FIDO	線上快速身分驗證
GDPR	通用資料保護法規
GPS	全球定位系統
GSMA	全球行動通訊系統
ICT	資訊和通訊技術
IAL1/2/3	身分保證等級（依 NIST 規定）
ID	身分
IDSP	身分服務提供者
IEC	國際電工委員會
INR.	建議注釋
IP	網際網路協定
ISO	國際標準化組織
ITU	國際電信聯盟
IVSP	身分驗證服務提供者
LoA	保證等級
MAC	媒體存取控制
ML	洗錢

MFA	多因素驗證
NGO	非政府組織
NIST	國家標準技術局
OIDF	OpenID 基金會
PII	個人身分資訊
PIN	個人身分證號碼
R.	FATF 建議
RBA	以風險為本的方法
SAG	標準諮詢小組
SCA	強式客戶身分驗證
TF	資恐
VASP	虛擬資產服務提供業
W3C	全球資訊網聯盟
UNHCR	聯合國難民事務高級專員

執行摘要

1. 數位支付規模以每年約 12.7% 的速度成長，預計 2020 年的年度交易量將達到 7,260 億筆。[1] 到 2022 年，估計全球 GDP 的 60% 將會數位化。[2]FATF 認為，為因應數位金融交易規模的成長，我們必須更加瞭解如何在數位金融服務領域中識別和驗證個人身分。數位身分（ID）技術正在迅速發展，使各種數位 ID 系統應運而生。本指引旨在協助政府、受監管實體 [3] 和其他利害關係方依據 FATF 第 10 項建議來判斷如何使用數位 ID 系統進行客戶審查（CDD）中的特定項目。

2. 若要應用本指引的以風險為本的方法，就必須瞭解數位身分識別系統的運作方式。指引的第二節扼要總結了數位 ID 系統的關鍵功能，詳細說明請見附錄 A。

---

1 凱捷（Capgemini）和法國巴黎銀行（BNP Paribas）（2018 年），*《2018 年世界支付報告》*，可透過以下網址在線上存取：https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf。

2 國際數據資訊（IDC），IDC FutureScape：全球 IT 產業 2019 年預測

3 在本指引中，「受監管實體」泛指金融機構、虛擬資產服務提供業（VASP）以及 FATF 標準所定義的指定之非金融事業或人員（DNFBPs），而 DNFBPs 必須在 R.22 指定的情況下進行客戶審查。2019 年 6 月，FATF 修訂第 15 項建議（新技術）和注釋 15，目的包括要求 VASP 必須履行第 10 項建議所規定的客戶盡職審查義務。

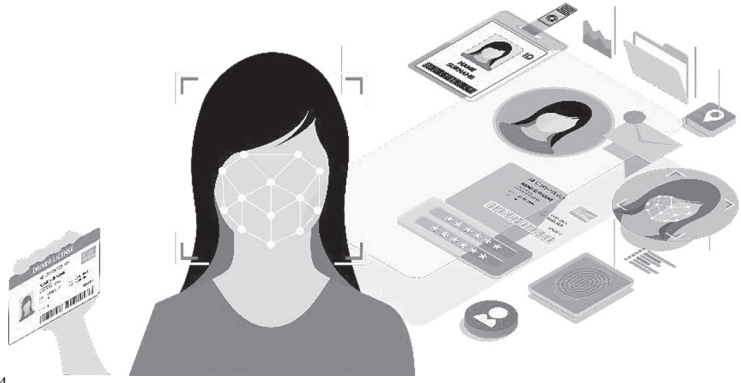
3. 第 3 節總結本指引涉及的主要 FATF 規定，包括使用「可靠、獨立」的原始文件、資料或資訊來識別和驗證客戶身分（第 10（a）項建議）。在數位 ID 的脈絡下，要求數位「原始文件、資料或資訊」必須具備「可靠、獨立」性質的意義在於：執行客戶審查所用的數位 ID 系統仰賴技術、適當治理、流程和程序，以適當確保系統得出可信的準確結果。本指引闡明，依賴可靠、獨立的數位 ID 系統，來為非親面對面自的客戶身分識別和交易提供適當風險緩解措施，可能得以將風險控制在標準等級，甚至更低。

建置可靠、獨立的數位 ID 系統來實作適當的風險緩解措施，可能得以將風險控制在標準程度，甚至更低。

4. 本指引所建議以風險為本的方法，遵循一套開源、共識導向的數位 ID 系統保證架構和技術標準（下稱「數位 ID 保證架構標準」），而此架構標準是在多個司法管轄區中所擬定。國際標準化組織（ISO）與國際電工委員會（IEC）正共同針對上述數位 ID 保證架構進行標準化，並更新一系列有關身分、資訊技術安全性、隱私的 ISO/IEC 技術標準，以期研擬一套全方位的全球數位 ID 系統標準。身分保證架構規定了不同「保證等級」的要求。保證等級衡量數位 ID 系統及其環節可靠性和獨立性的可信度。雖然各司法管轄區所訂保證等級在某些方面可能不同，但是為了便於參考，本指引主要參考美國國家標準技術研究院（NIST）的數位 ID 保證架構標準

（下稱 NIST 數位 ID 指引）[4] 以及歐盟的 e-IDAS 法規。[5] 司法管轄區應根據其國內數位 ID 保證架構及其他相關技術標準來考慮本指引所述方法。[6]

5. 「數位 ID 保證架構標準」與「防制洗錢 / 打擊資恐法規」的來源和目標受眾皆有不同。本指引銜接了數位身分保證架構標準以及 FATF 客戶審查規定。如下表所示，數位 ID 系統的關鍵環節與第 10（a）項建議中的特定識別和驗證要求有關。因此，數位 ID 保證架構和技術標準不僅定義了這些環節並設定各個保證等級的要求，亦供了非常實用的評估工具，可據以判斷數位 ID 系統在防制洗錢 / 打擊資恐方面的可靠性和獨立性。



4 NIST 800-63 數位身分指引包含一系列文件：NIST SP 800-63-3 數位身分指引（概述）；NIST SP 800-63A：數位身分指引：註冊和身分證明；NIST SP 800-63B 數位身分指引：驗證和生命週期管理；以及 NIST SP 800-63C 數位身分指引：聯合識別及判斷提示。

5 歐盟第 910/2014 號規章「電子交易在內部市場的電子身分識別驗證和信託服務規則」。

6 司法管轄區可能沒有數位 ID 保證架構或數位 ID 系統專屬的技術標準，但可能訂有其他技術標準（例如高度相關的 IT 客戶資料保密標準）。

客戶盡職審查規定（自然人）	數位 ID 系統的關鍵環節
識別 / 驗證 –R.10（a）	身分證明和註冊（綁定）– 您是誰？取得屬性（名稱、DoB、ID 編號等）及其證據；確認並驗證 ID 證據，並將其解析連結至唯一證實身分的個人。 綁定 - 核發憑證 / 驗證機制，將憑證的持有 / 控制者連結至證實身分的個人 身分驗證 – 您是否為已識別 / 驗證身分的個人？確定申請者持有並控制綁定憑證。若受監管實體執行身分識別 / 驗證，確認潛在客戶持有既存的數位 ID 憑證，則此驗證機制適用於 10（a）。

6. 本指引表明（1）身分驗證與 R.10（a）有關，其中受監管實體使用既存的數位 ID 憑證為客戶開設帳戶（並非內部數位 ID 解決方案），而且（2）在數位金融和數位 ID 脈絡下，有效地驗證客戶身分以授予帳戶存取權限，有助於支持防制洗錢 / 打擊資恐工作。

7. 第 5 節是本指引的重點，旨在為政府主管機關、受監管實體和其他利害關係方提供指引，說明如何依據第 10 項建議，透過以風險為本的方法，採用數位 ID 系統來識別並驗證身分，以支持第 10（d）項建議所述的現行

以風險為本的方法採用數位 ID：（1）瞭解數位身分識別系統的保證等級，並且（2）根據特定保證等級來評估 ID 系統就洗錢 / 資恐風險而言是否具有適當的可靠性和獨立性

盡職調查。建議採用技術中立方法（即不偏好任何特定類型的數位 ID 系統）。此方法具有兩個要素：

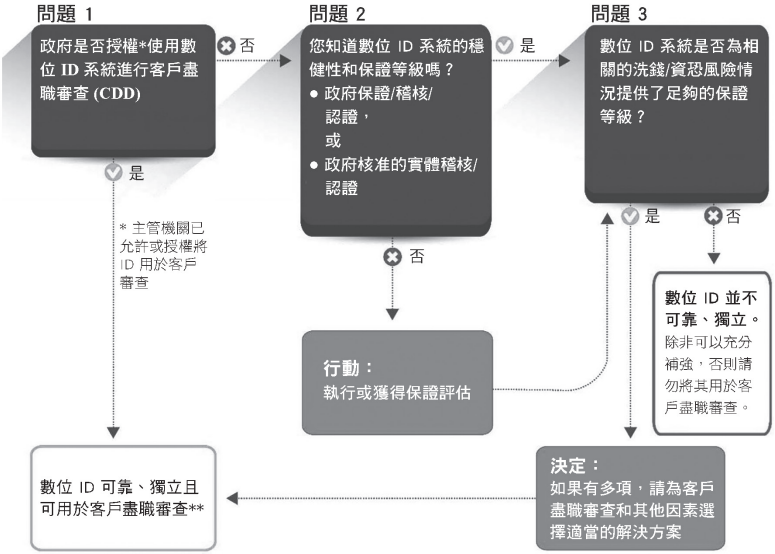
a. 瞭解數位 ID 系統主要環節（包括其技術、架構和治理）的保證等級，確認其是可靠、獨立的資訊源；以及

b. 針對，判斷潛在的洗錢、資恐、詐欺及其他非法融資風險，依照特定數位 ID 系統既有的保證等級，判斷其是否具有適當程度的可靠性和獨立性，足以支持重大的洗錢、資恐、詐欺及其他非法融資風險防治工作。

8. 第 5 章介紹如何利用數位 ID 保證架構標準來評估可靠性 / 獨立性。該節亦載明受監管實體的決策流程作為參考指引，可據以判斷使用數位 ID 來執行客戶審查的特定項目是否符合 FATF 第 10 項建議之規定。政府和受監管實體必須依據司法管轄區和個別實體的具體情況來調整此決策流程。根據特定轄區的數位 ID 系統和法規架構，政府和受監管實體在評估身分系統的保證等級及其對客戶審查的適用性方面，可能各具不同的角色和責任，如下列決策流程圖所示。

9. 本指引並不具約束力，僅闡明現行的技術中立 FATF 標準。

圖 1 受監管實體的決策流程



** 在 R.10 中需要其他資訊，且可能需要其他風險緩解措施

10. 本指引第 4 章探討數位 ID 系統的若干效益及風險。數位 ID 系統涉及的許多風險同樣存在於實體 ID 之中。但是，透過開放式通訊網路（網際網路）進行身分證明及 / 或驗證，會對數位 ID 系統造成特定風險，尤其是網路攻擊和潛在的大規模身分盜竊。另一方面，數位 ID 系統若能依據數位 ID 保證架構標準來減輕相關風險，可望大幅加強客戶審查和防制洗錢 / 打擊資恐控管、提升金融普惠性、改善客戶體驗，以及降低受監管實體成本。

11. 本指引重點介紹使用客戶審查數位 ID 系統的多種方式，及其如何促進金融普惠發展。首先，數位 ID 系統可以使政府採取更靈活、精細和前瞻性的方法來建立所需的屬性、身分證明及正式身分證明流程，包括在引導時採用有助於金融普惠的方式識別和驗證客戶身分。其次，數位身分保證架構標準本身為身分證明及個人身分驗證流程提供一定的靈活性，且可針對金融普惠目標加以量身定製。最後，監理機關和受監管實體採用以風險為本的客戶盡職審查方法有助於金融普惠發展，其中包括依照 2017 年 FATF 客戶審查和金融普惠增補規定來使用數位 ID 系統。

給政府主管機關的建議

12. 受監管實體應制定明確的指引或規定，依據適當、風險導向的方式使用可靠、獨立的數位 ID 系統來防制洗錢 / 打擊資恐。首先，請瞭解司法管轄區可用的數位 ID 系統及其如何滿足客戶身分識別和驗證、持續盡職調查（以及相關記錄保留和第三方信賴要求）的要求和指引。

13. 評估所有相關機構中有關客戶審查的現行法規和指引是否適用數位 ID 系統，並依據司法管轄區脈絡與身

分生態系予以適當修訂。例如主管機關應考慮釐清，若能使用適當保證等級的數位 ID 系統來識別 / 驗證和鑑定遠端客戶身分，可將非面對面的引導風險控制在標準程度，甚至可將客戶審查風險降至低度。

14. 進行客戶盡職審查時，應採用原則、績效及 / 或結果導向的標準來確立必要的屬性、證據和流程，據以證明正式身分。鑑於數位 ID 技術的快速發展，這將有助於推廣盡責的創新模式並因應未來的法規要求。

15. 採用政策、法規、監督和檢查程序，支援受監管實體研擬有效、整合的「以風險為本」方法，運用資料流量、技術架構和流程來控管所有相關的數位 ID、防制洗錢 - 打擊資恐、反詐欺和一般性攻擊威脅，強化所有與風險相關的功能。

16. 開發整合式的多重利害關係人方法，以瞭解數位 ID 涉及的機會和風險，並制定相關法規和指引以減輕風險。評估並斟酌利用負責身分、網路安全 / 資料保護和隱私（包括技術、安全性、治理和資源方面）等事宜之主管機關所採行的既有數位 ID 保證架構和技術標準，據以評估客戶審查所用的數位 ID 系統保證等級。根據 FATF 第 2 項建議，與相關機構協調合作，以促進一種全面、協調的方式來瞭解和因應數位 ID 生態系統中的風險，並確保「防制洗錢 / 打擊資恐規定」與「資料保護和隱私規則」兩者的數位 ID 系統

彼此相容。

17. 防制洗錢 / 打擊資恐機構可以考慮採用各種機制，以加強與私營部門利害關係方（包括受監管實體和數位 ID 服務提供者）交流與合作，以利找出身分驗證方面的關鍵契機、風險和緩解措施。相關機制可能包括法規「沙盒」方法，提供受監管的環境來測試數位 ID 系統如何與國家防制洗錢 / 打擊資恐法律和法規交互搭配作用。主管機關也可以考慮開發相關機制，以促進跨產業合作、識別並解決現有數位 ID 系統中的漏洞。

18. 考慮依據透明化的數位 ID 保證架構和技術標準來進行稽核和認證，或核准專家機構來執行這些功能，藉以支持可靠、獨立的數位 ID 系統的開發和實施。如果主管機關本身不對 IDSP 進行稽核或提供認證，則建議其可交由適當的專家機構支援品保測試和認證工作[7]，以利在司法管轄區中提供可信的認證。鼓勵主管機關支援數位 ID 保證架構標準的協調工作，以針對數位 ID 系統的「可靠、獨立」性質達成共識。

19. 採用適當的數位 ID 保證架構和技術標準來研擬和實施政府提供的數位 ID 系統。主管機關的數位 ID 系統

---

[7] 這些專家認證機構可以為特定轄區或地區提供服務，也可以在國際提供服務。

運作方式和保證等級應維持公開透明。

20. 鼓勵透過靈活、以風險為本的方法來使用客戶審查的數位 ID 系統，以利促進金融普惠發展。應考慮提供相關指引，明定如何使用不同保證等級的數位 ID 系統，來進行分層客戶盡職審查的身分證明 / 註冊和身分驗證。

21. 監控數位 ID 領域的發展，以期在國內外分享知識、最佳實務並確立法律架構，促進盡責創新模式，並提升數位 ID 系統的靈活性、效率和功能。

給受監管實體的建議

22. 瞭解數位 ID 系統的基本組成，尤其是身分的證明、驗證及其如何應用於所需的客戶審查項目（請參閱第 2 章和附錄 A）。

23. 採取以風險為本的方法來使用客戶審查的數位 ID 系統，其中包括：

    a. 瞭解數位 ID 系統的保證等級，尤其是在身分證明和驗證方面，以及

    b. 確認保證等級適用於客戶、產品、司法管轄區、地理範圍等相關的洗錢 / 資恐風險。

24. 在洗錢 / 資恐風險較低的情況下，應考慮較低保證等級的數位 ID 系統是否足以用於精簡的盡職調查程序。

例如若情況允許，可採用分層客戶盡職審查方法不同保證等級的數位 ID 系統，以利促進金融普惠發展。

25. 如果內部政策或慣例一律將非面對面的業務往來或交易歸類為高風險活動，請考慮對這些政策進行審查和修訂，採用獨立數位 ID 系統的適當風險緩解措施以實現可靠的客戶身分識別 / 驗證機制，如此可將風險控制在標準程度，甚至更低。

26. 必要時，可使用反詐欺和網路安全流程來支援防制洗錢 / 打擊資恐工作的數位身分證明及 / 或驗證機制（引導階段的客戶身分識別 / 驗證以及現行的盡職調查和交易監控）。例如，受監管實體可以利用數位 ID 系統內建的防護措施來防止詐欺（監控身分驗證事件，偵測數位 ID 遭系統性濫用存取帳戶的行為，包括遺失、洩露、竊取或出售數位 ID 憑證 / 驗證機制），並將此資料饋入系統進行持續盡職調查，以及監控、偵測可疑交易並通報主管機關。

27. 受監管的實體應確保設有存取管道或流程可供主管機關獲取身分識別和驗證所需的基本身分資訊、證據或數位資訊。鼓勵受監管實體、主管機關、政策制定者及數位 ID 服務提供者合作，探討如何在數位 ID 環境中有效率地實現此目標。

給數位 ID 服務提供者的建議[8]

28. 瞭解客戶盡職審查的防制洗錢 / 打擊資恐要求（尤其是客戶身分識別 / 驗證和現行盡職調查）及其他相關法規，包括受監管實體保留客戶審查記錄的要求。
29. 尋求政府或經認可的專家機構進行保證測試和認證，若國內無適用機構，則尋求其他國際知名專家機構執行。若條件允許，可參與公部門法規「沙盒」（或其他相關機制）以評估數位 ID 系統的保證等級。
30. 向防制洗錢 / 打擊資恐所監管的實體提供透明資訊，列出有關身分證明、驗證及適用的聯合識別 / 互通性的數位 ID 系統保證等級。

[8] 雖然 FATF 標準僅適用於受監管實體（即金融機構、虛擬資產服務提供業及指定之非金融事業或人員），但數位 ID 服務提供者亦可參考本指引，以期在為受監管實體提供服務時能達成 FATF 的要求。最終，受監管實體有責任達成 FATF 的要求。

31. 防制洗錢金融行動工作組織（FATF）致力於確保全球防制洗錢 / 打擊資恐（AML/CFT）標準可促進盡責的金融創新模式。在這方面，FATF 大力支持在金融領域採用新技術，來配合並強化防制洗錢 / 打擊資恐標準和金融普惠目標。[9]

32. 數位身分（ID）領域創新的快速發展已來到轉捩點。數位 ID 的標準、技術和流程已發展到一定程度，目前的數位 ID 系統已十分普遍或即將大量上市。其中若干相關技術包括：各種生物辨識技術；幾乎無所不在的網際網路和行動電話（包括附相機、麥克風和其他智能技術的「智慧型電話」迅速發展和普及）；數位裝置識別碼和相關資訊（例如 MAC 和 IP 位址、[10] 手機號碼、SIM 卡、全球定位系統（GPS）地理位置）；高畫質掃描機（用於掃描身分證、駕照和其他文件）；高解析度視訊傳輸（支援遠端識別和驗證以及「活體」證明）；人工

創新的快速步伐已來到轉捩點 ... 數位 ID 系統目前十分普遍，或即將大量上市。

9 請參見 FATF *對於金融科技和監理科技的立場*（2017 年 11 月 3 日），*網址為* www.fatf-gafi.org/publications/fatfgeneral/documents/fatf-position-fintech-regtech.html。

10 MAC 位址識別裝置、IP 位址識別連線。

智慧 / 機器學習（例如用於確認政府核發身分證的有效性）；以及分散式分類帳技術（DLT）。

潛在效益

33. 符合高科技、組織和治理標準的數位 ID 系統具有廣闊前景，可望在數位時代全球經濟的各種環境（例如全球的金融服務、醫療和電子政務）增進自然人身分識別的可信度、安全性、隱私和便利性。這些數位 ID 依預設具有較高保證等級。

34. 關於 FATF 標準，適當可靠的獨立數位 ID 系統可以：

- 在引導階段加速識別和驗證客戶身分
- 在整個業務往來流程中支援現行盡職調查和交易審查，
- 促進其他客戶盡職審查（CDD）措施，以及
- 交易監控輔助機制，用於偵測和通報可疑交易及一般風險管理和詐欺防制。

35. 這些機制亦可降低受監管實體的成本並提高其效率，有利於資源重新分配給其他防制洗錢 / 打擊資恐部門。

36. 可靠、獨立的[11]數位 ID 系統亦有助於在各種條件下（包括偏遠地區）證明正式身分，支援服務短缺的民眾證明正式身分以取得受監管的金融服務，從而促進金融

---

[11] 為求閱讀方便，特定情況下「可信賴」一詞用作「可靠、獨立」的同義詞。

普惠發展。促進受監管金融部門的普及化，可進一步加強防制洗錢／打擊資恐的保障措施。

潛在的風險

37. 數位身分識別系統也會帶來洗錢 / 資恐方面的風險，必須詳加瞭解和予以減輕。若受監管實體未能做到這一點，也將無法符合第 10（a）項建議及 FATF 標準規定，其要求受監管實體著眼於新型與既有產品採用新型或開發中技術的情形，從中識別、評估並減輕其在金融市場中可能引發的洗錢或資恐風險。[12]

38. 這些風險將於第 4 章詳述。大規模數位 ID 系統若未達到適當保證等級，則會構成網路安全風險，包括無法有效防範網路攻擊，導致金融部門大範圍停擺或使數位 ID 系統本身失效。這類狀況也會帶來重大的隱私、詐欺或其他相關金融犯罪風險，因為網路安全漏洞可能導致大量身分盜用，進而危及個人身分資訊（PII）的安全。[13] 治理、資料安全和隱私相關風險也會影響防制洗錢 / 打擊資恐措施的成效。這些風險因數位 ID 系統的環節而異，但由於潛在的攻擊規模，破壞性較傳

---

12 R.15（用於金融機構和 VASP）和 R.22（用於指定之非金融事業或人員）。

13 **PII** 包含任何可以單獨或與其他資訊結合使用以識別特定個人身分的資訊。

統 ID 系統相關的漏洞更大。技術上的進步及精心設計的身分證明和驗證流程皆有助於減輕這些風險，如第 4 節所述並將於第 5 節進一步討論。

39. FATF 了解數位 ID 系統的潛在風險和收益，因此制定本指引以闡明如何使用數位 ID 系統來遵守該標準所述特定防制洗錢 / 打擊資恐要求。

宗旨和目標受眾

40. 本指引旨在幫助政府機構更清楚瞭解數位 ID 系統的運作原理，並闡明如何在全球防制洗錢 / 打擊資恐標準下予以應用。這包括決策者、監理機關、受監管實體的監督者和檢查員；隱私、資料保護和網路安全機構（若相關）；以及其他訂有相關政策目標（例如促進金融普惠性）的政府機構。

41. 本指引另一項目標為協助私營部門的利害關係方，包括受監管的實體和數位 ID 服務提供者。同時亦涉及到國際組織、非政府組織（NGOs）及其他在金融服務及人道援助中提供和使用數位 ID 系統的組織。

範圍

42. 本指引的重點是將第 10 項建議（客戶審查）實施於客戶引導（開戶）階段（依第 10[a] 項建議），據以採用數位 ID 系統來進行身分識別 / 驗證流程。本文件檢視了數位 ID 在第 10（d）項建議下支援現行盡職調查（包

括交易監控）的潛力，亦說明受監管實體採用第 17 項建議（第三方信賴），彼此提供數位 ID 系統以識別 / 驗證客戶身分的情形。

43. 根據技術中立的原則，第 11 項建議（記錄保存）規定同樣適用於數位和實體（文件）形式的記錄保存。在實務上，數位 ID 系統可能的問題在於如何保留和存取所需的客戶審查資訊，以支援受監管實體遵守第 11 項建議的要求。在數位 ID 的脈絡下，保存記錄的方法各有不同，取決於數位 ID 系統的類型和設計、其元件提供者的類型和職責，以及司法管轄區內的相關監管和承包架構。例如，當政府提供數位 ID 系統時，它們會蒐集或產生用於身分證明 / 註冊的基本身分證據（原始文件、資訊和資料），因此可以監管或執法目的存取此資訊，進而達成 R.11 所規定的目標。如果受監管實體使用非政府提供者提供的數位 ID 系統，基本身分證據可以全部或部分由數位 ID 服務提供者（IDSP）及 / 或其他實體保留。另外，私營部門數位 ID 服務提供者可以直接從數位來源（例如政府資料庫或私營部門公用事業記錄）取得 / 確認部分或所有基礎身分資料。在此情況下，用於指明特定身分證據類型的數位記錄，包括資料來源、日期 / 時間和獲取方式，皆可能符合第 11 項建議 11 的要求。上述問題已由主管機關藉由其防制洗錢 / 打擊資恐和數位 ID 監管架構、並

由受監管實體透過標準代理機構及金融服務提供者的承包關係予以處理。因此，本指引不再進一步說明記錄保存及該等要求。

44. 本指引著重於個人（自然人）客戶的身分識別。本指引不探究數位 ID 系統用於輔助識別和驗證法人客戶的法人代表身分、輔助進行客戶審查流程其他項目等用途，尤其是根據第 10 項建議（b）識別和驗證實質受益人的身分，或根據第 10 項建議（c）瞭解並獲取有關業務往來目的和意圖的資訊；然而，可靠、獨立的數位 ID 系統對於上述客戶審查功能都很重要。

45. 本指引涵蓋由政府自行或授權[14]提供及由私部門提供的數位 ID 系統。在政府提供的數位 ID 系統方面，本指引著重於通用數位 ID 系統（即在司法管轄區內可用於證明所有或多數用途的有效正式身分證明），雖然本指引也探討限定用途的身分證明（即在特定用途才有效的身分證明），例如社會保險碼或其他資料庫，前提是政府授權將其用於客戶審查並提供給受監管實體和數位 ID 服務提供者。第 2 章進一步說明本指引涵蓋的數位 ID 系統類型。

---

[14] 若政府與諸如 UNHCR（聯合國難民署）等國際組織或其他實體締約，或以其他方式安排或授權該等實體提供並運作數位 ID 系統，則該系統將以「政府授權」的名義供應各界使用。在上述身分識別功能中，非政府角色代替了政府。

46. 本指引未確立用於評估數位 ID 系統技術、流程和架構獨立性或可靠性的保證架構或技術標準。相反，其仰賴由其他組織和不同司法管轄區所開發的數位 ID 保證架構和技術標準（稱為數位 ID 保證架構標準）。有關技術標準說明請參見第 2 節，詳細資訊請參見第 5 章和附錄 E。

47. 本指引包括五份附錄和一份詞彙表，以及相關的進一步文獻資料：

- *附錄 A：基本數位身分系統及其參與者之說明*：更詳細概述第 5 章有關數位 ID 系統環節的概念。
- *附錄 B：案例研究* – 提供了在不同司法管轄區使用的數位 ID 的範例，包括客戶盡職審查和金融服務的使用。
- *附錄 C：身分識別永續發展原則* – 強調各司法管轄區和組織正在處理的治理 / 當責、隱私和其他營運問題。[15]
- *附錄 D：數位 ID 保證架構和技術標準制定機構* - 列出許多相關數位 ID 保證架構標準的標準制定機構（不包括國家或地區機構）。
- *附錄 E：美國和歐盟數位 ID 保證架構和技術標*

---

15 上述原則係透過協作流程制訂，已獲 25 個發展合作夥伴、國際組織、非政府組織、私營部門協會和政府實體的認可。

準概述 - 詳述國家和地區數位 ID 保證架構，例如美國和歐盟等地。

- *詞彙表* - 本指引使用的數位 ID 術語說明。

第 2 章：數位 ID 術語和關鍵特徵

在本指引中，「身分」是什麼？

正式身分概念

48. 身分是具有許多含義的複雜概念。就 FATF 涉及 10（a）項建議之目的，即「識別客戶並驗證客戶身分」而言，「身分」是指正式身分，有別於非正式用途的廣義個人和社會身分概念（例如個人或網路上未受監管的點對點商業或社交互動）。本指引涵蓋數位 ID 系統用於證明金融服務對象「正式身分」的用途。

49. 在本指引中，[16] **官方身分**是唯一自然人的限定概念：

a. 其基礎為某些個人特徵（屬性或識別符），可在群體或特定環境脈絡中確立該人的獨特性，以及

b. 由國家基於監管和其他正式用途所認可。

正式身分證明

50. **正式身分認證**通常取決於政府提供或核發的某種註冊、文件或認證（例如出生證明、身分證或數位 ID 憑證），其構成了核心屬性（例如姓名、出生日期和地點）的證據，用於確立和驗證正式身分。

使用結果導向方法確立身分屬性有利於司法管轄區因應正式身分證明程序的未來需求

51. 證明「正式身分」的標準可能因司法管轄區而異。政府行使主權時，會確立正式身分證明所需的屬性、證據和流程，這些因素會隨著時間而改變。隨著身分認同的技術和文化概念的發展，政府可能會授權使用各種不同的屬性。在確立正式身分證明的標準時，政府可以使用固定、規定性、規則導向的方法，也可以使用原則、績效及 / 或結果導向的方法。後一種方法較為靈活。鑑於數位 ID 技術和標準的快速發展，其有利於司法管轄區因應正式身分證明程序的未來需求，並支持盡責的創新模式。

---

[16] 在本指引中，FATF 使用此定義無意限制其他標準制定機構（ssb）的不同定義。

52. 歐盟遵循通用保證架構，使成員國得以適應不同國家要求，例如接受各國適用的不同類型正式身分證明文件和程序，前提是結果符合 eIDAS 架構中的要求。取決於需要驗證身分的領域，授權來源可能具有多種形式，例如登記處、文件和相關機構等。即使在相似背景下，各個歐盟成員國的授權來源也可能有所不同，但是 eIDAS 架構允許協調和交叉認可。國際標準化組織（ISO）[17] 目前正在制訂全球標準，用於識別金融服務對象的自然人，亦適用於數位化的環境。

53. 在許多國家，正式身分證明是透過**通用 ID** 系統（有時稱為基本 ID 系統）提供，例如國家身分證和民事登記系統。這類系統通常提供文件及 / 或數位憑證，受到政府機構和私營部門服務提供者廣泛認可並接受，用作各種目的正式身分證明。並非所有司法管轄區皆有通用 ID 系統。

54. 司法管轄區通常也有各種**「限定用途」ID** 系統（也稱為功能型 ID 系統），旨在為特定服務或部門（例如稅務管理）提供識別、驗證和授權功能；取得特定政府福利和服務；表決；授權操作機動車輛；（在特定司法管轄區）取得金融服務等。限定用途身分證明的範例包括（但不限於）：稅籍號碼、駕駛執照、護照、

---

[17] ISO 標準諮詢小組（SAG）第 68 技術委員會第 7 工作小組

選民登記卡、社會保險碼和難民身分證明文件。特定情況下，尤在是缺少通用 ID 系統的國家中，此類功能系統和憑證也可用於提供正式身分證明。

55. 正式身分證明通常由政府（或代表政府）提供。在數位時代，新的模式開始問世，由私營部門自行或合作提供的數位憑證已獲政府認可為網路環境中的正式身分證明（例如丹麥的 NemID），另也有政府所核發較傳統的數位憑證（例如電子國民身分證）。

56. 至於難民的正式身分證明，也可以由負有相關職責的國際公認組織提供。[18] 請見說明欄 8。

本指引所謂的數位 ID 系統是什麼？

57. 數位 ID 系統會採用電子方式在網路（數位）及 / 或現場環境提供各種保證等級的個人正式身分。

58. 本指引著重於端到端數位 ID 系統（即涵蓋身分證明 / 註冊和驗證流程的系統）。數位 ID 系統可能涉及不同的運作模式，並且可能仰賴各種實體和技術、流程和架構類型。本指引提及的數位 ID 系統是指整體系統，而非組成部分。

59. 數位 ID 系統的環節未必都是數位性質。身分證明和註冊環節的特定元素可以是數位或實體性質（文件），

---

[18] 請參閱 1951 年《難民地位公約》第 25 條、第 27 條和 1950 年《聯合國難民事務高級專員公署條例》。

也可以是兩者的組合，但是**綁定、憑證、身分驗證和可攜權 / 聯合識別（若適用）必須是數位性質**。下一節將進一步說明這些概念。

60. 數位 ID 系統可能以各種方式運用數位技術，例如但不限於：

- 電子資料庫、包括分散式分類帳，用以獲取、確認、儲存及 / 或管理身分證明文件
- 用於驗證身分以存取行動裝置、線上和線下應用程式的數位憑證
- 用於識別及 / 或驗證個人身分的生物辨識技術，
- 數位應用程式介面（API）、平台和協定，用於促進線上身分識別 / 確認以及身分驗證。

數位 ID 系統的關鍵組成部分是什麼？

61. 正如 NIST 數位 ID 指南所述，**數位 ID 系統**包含兩項基本環節及一項選擇性的第三環節，如下所述。子環節可能交由不同實體負責運作，包括公私部門的混合編制實體。不同司法管轄區和組織使用的術語可能略有不同，依本文所述系統而定。各階段的詳細說明收錄於***附錄 A：基本數位身分系統及其參與者之說明***

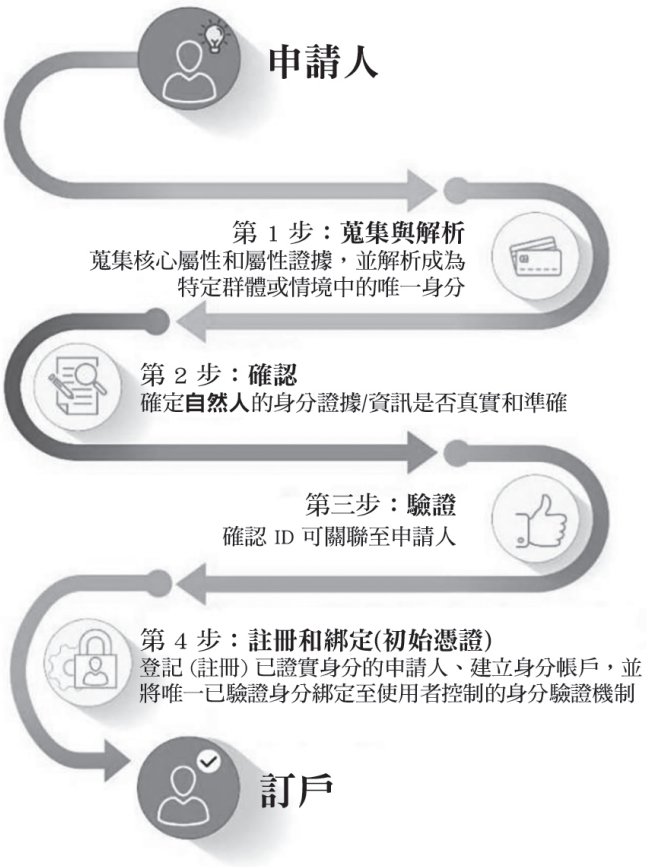
環節一：身分證明和註冊（含初始綁定 / 憑證）（必要）

62. 此環節釐清下列問題：**您是誰？**且涉及蒐集、確認和驗證身分證據及相關個人資訊；建立身分帳戶（註冊）

並將個人唯一身分綁定至此人持有和控制的驗證機制。

63. 此環節直接且最密切地關聯到 R.10（a）的識別 / 驗證要求（見第 3 節）。

圖 2 身分證明和註冊



注意：此圖僅用於說明，身分證明和註冊的階段順序可能不同。此流程旨在是識別和驗證個人身分，並將其綁定至身分驗證機制。另請參閱附錄 A，以進一步瞭解此圖使用的關鍵術語。

64. 在「環節一」中可以採取的行動範例如下（僅供示意）：

- 蒐集：親自及 / 或在線上出示和蒐集身分屬性和證據（例如填寫線上表格、發送自拍照片、上傳文件照片（例如護照或駕照等））。
- 驗證：進行數位或實體檢查，以確認文件真實性及其資料或資訊的準確性（例如檢查實體安全性功能、到期日期，以及使用其他服務來驗證屬性）。
- 重複資料刪除：確認身分屬性和證據關聯到 ID 系統中的唯一身分（例如採用重複記錄搜尋、生物辨識及 / 或重複資料刪除演算法）。
- 驗證：將個人連結到所提供的身分證據（例如使用生物辨識解決方案，如臉部識別及生命偵測等）。
- 註冊身分帳戶和綁定：建立身分帳戶並核發一或多項身分驗證機制，並將其連結至該身分帳戶（例如密碼、手機上的一次性密碼 [OTC]、PKI[19] 智慧卡、FIDO 憑證等）。此流程會啟用驗證機制（請參見下文）。

---

19 公開金鑰基礎架構

環節二：身分驗證及身分生命週期管理（必要）

65. 身分驗證釐清下列問題：**您是否為已被識別和驗證身分的當事人？**此環節依據驗證機制的所有權和控制權，來確認主張身分者（在引導流程中的客戶或申請者）與已證實且註冊身分者為同一人。

66. 有三種因素可用於進行身分驗證（請參見下方圖 3）：（1）所有權因素（您擁有的事物，例如加密金鑰）（2）知識因素（您知道的東西，例如密碼）；（3）固有因素（您的特徵，例如生物辨識資訊）。[20]

67. 身分驗證可憑藉各種驗證因素、協定或流程來進行。這些驗證因素具有不同的安全等級 - 請參閱第 5 章有關身分驗證風險的討論；一般認為單一身分驗證因素不夠可靠。採用多種驗證因素的身分驗證流程通常公認較為穩健可靠。[21]

---

20 本指引所述身分驗證構件有別於歐盟法律架構下的「強式客戶身分驗證（SCA）」。依歐盟指令（EU）2015/2366（PSDII）規定，有效 SCA 因素的構成條件必須根據 PSDII 及 PSDII 所規定的「強式客戶驗證及安全通訊之監管技術標準」（RTS on SCA & CSC）予以鑑定，而非 FATF 指引。

21 隨著數位 ID 系統的發展，相關知識也更加精細入微。在持續作用的驗證機制中，驗證強度的評估標準有時不在於驗證因素的多寡，而是取決於使用多種動態、數位客戶資料來源而產生的整體穩健性，包括預定的登入管道、地理位置、使用頻率、使用類型、IP 位址、生物力學度量行為模式

圖 3 通用驗證因素

說明欄 1 身分驗證在客戶盡職審查和其他防制洗錢 / 打擊資恐措施中的作用

- 如果個人身分被證實並註冊數位 ID 系統，即可使用綁定身分的憑證及身分驗證機制，將該身分「判斷提示」給第三方的「信賴方」（例如受監管實體）。身分證明和註冊流程的強度可為信賴方提供身分資訊真實性的可信度（例如姓名和年齡等

屬性正確且可關聯至真實個人），且身分驗證流程可讓信賴方確保憑證的提供者和持有者是同一人，而非竊賊或冒名頂替者。因此，數位 ID 驗證系統的重要功能在於驗證個人身分，而且可供受監管實體用於開設帳戶的客戶盡職審查流程。

- 請注意，對現有客戶的「身分驗證」也是現行盡職調查和授權帳戶存取的重要安全措施。在特定情況下，受監管實體可透過開立帳戶所用的相同數位 ID 憑證和身分驗證服務來授權帳戶存取，但未必總是如此。例如，許多受監管實體會發布自有的憑證 / 身分驗證機制（例如用於登入線上帳戶的 PIN 和權仗）及 / 或將其連結到行動電話或瀏覽器內建的裝置身分驗證機制（例如使用 FIDO 標準）。

68. **身分生命週期管理**是指因應身分生命週期中可能發生的事件而應採取的行動，這些事件會影響身分驗證機制的使用、安全性和可信度，例如**驗證機制**及 / 或**憑證**的遺失、遭竊、未經授權的複製、到期和註銷。

環節三：可攜權和互通性機制（非必要）

69. 數位 ID 系統也可能包含特定環節，由其支援身分證明的可攜功能。可攜式身分是指個人的數位 ID 憑證可

在無關聯的公私部門實體業務往來中用於證明正式身分，而無需每次都要取得和驗證個人資料並進行客戶識別 / 驗證。可攜權可由不同的數位 ID 架構和協定予以支援。在歐洲，eIDAS 法規提供一項數位 ID 系統的交叉識別架構。

70. 聯合識別是一種允許正式身分可攜權的方法。聯合識別是指使用聯合架構和判斷提示協定*在一組網路系統之間*傳遞身分和身分驗證資訊，支援橫跨不同網路的互通性。在英國，GOV.UK Verify 是聯合識別數位 ID 的範例 – 參見說明欄 16

數位 ID 保證架構和技術標準

71. 數位 ID 技術、流程和架構可靠性的保證架構和技術標準已經或正在由以下單位研擬：

- 各司法管轄區或超國家司法管轄區（例如歐盟、加拿大和澳洲）
- 國際標準組織或特定產業組織，例如國際標準化組織（ISO）、國際電工委員會（IEC）、線上快速身分驗證（FIDO）聯盟、OpenID 基金會（OIDF）、國際電信聯盟（ITU）和 GSMA。

72. 請參見***附錄 D：數位 ID 保證架構和技術標準制定機構***，此資料總括介紹了這些組織的梗概。

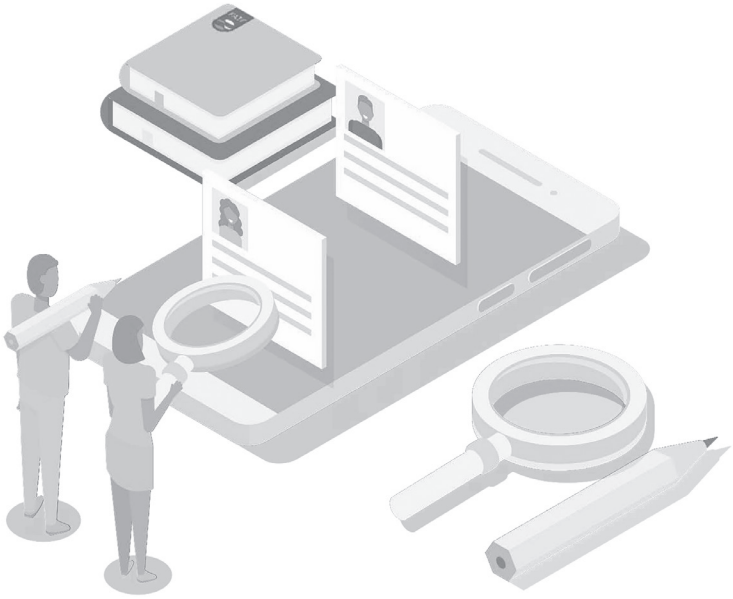
73. 目前，各個司法管轄區研擬的數位 ID 保證架構標準

採用不同的編號及 / 或名稱來表示保證等級，但是在本質上大致相同。目前，各個司法管轄區正在對映彼此的數位 ID 技術標準，以解決尚未統整的差異。在 2018 年，ISO 與國際 IEC 共同發布一項自然人身份證明和註冊的國際標準（ISO/IEC 29003：2018）。ISO 目前正在修訂實體身分驗證保證架構（ISO/IEC 29115：2013），並著手採用其風險管理指南（ISO 31000：2018）來因應身分相關風險。此外，ISO 正在努力更新、調整並同步所有其他 ISO 標準，以建立一套全方位國際數位 ID 保證架構。

74. 有鑑於標準不斷演進，本指引引述大量 NIST 數位 ID 指引和 eIDAS 架構。防制洗錢 / 打擊資恐主管機關應與數位 ID、網路安全和其他相關機構的對等單位密切合作，以提出適用的數位 ID 保證架構標準。

75. 隨著數位 ID 技術、架構和流程的發展，數位 ID 系統本身的保證架構和技術標準也需與時俱進，且可能會落後於數位 ID 系統的演進速度。敦促公私部門密切追蹤新興的數位 ID 技術 / 流程，可提供更強大的身分證明或身分驗證，並將架構標準視為實用評估工具，而非使用現有的更高保證等級來確立上限。

第 3 章：客戶盡職審查標準



76. 本章讀者必須對數位 ID 系統的運作原理具有基本瞭解。建議讀者複習第 2 章和附錄 A 有關通用數位 ID 系統基本步驟的簡要說明，為本節有關第 10 項建議的運作方式（尤其是其「可靠、獨立」標準）提供討論基礎。

77. 依第 10 項建議要求，司法管轄區必須規定受監管實體執行客戶盡職審查（CDD）義務。以下討論闡明第 10（a）項建議在數位 ID 系統中的應用。受監管實體必須根據第 10 項和第 1 項建議的註釋，使用以風險為本的方法（RBA）來確定客戶審查措施的範圍。本節也

簡要說明可靠的數位 ID 系統如何達成「建議」所列的其他防制洗錢 / 打擊資恐要求。

客戶識別 / 驗證規定（引導階段）

78. 在與客戶建立業務關係時（即引導階段），受監管實體需要*使用可靠、獨立的原始文件、資料或資訊*來識別和驗證客戶身分」（第 10 項建議，（a）子節））。

書面或數位形式的身分證明文件和流程

79. 第 10 項建議屬於技術中立性質。第 10（a）項建議允許金融機構使用「文件」以及「資訊或資料」來識別和驗證客戶身分。第 10（a）項建議並未限制身分證據（「原始文件、資訊或資料」）的形式（文件 / 實體或數位）。

80. 此外，雖然第 10（a）項建議確實要求金融機構以某種「可靠」的方式將客戶已證實的身分連結到個人，但 FATF 標準未規定引導階段的身分識別 / 驗證流程，應如何將已驗證的客戶身分連結到唯一、真實的個人。因此就該目的而言，第 10 項建議並未對數位 ID 系統的使用設下限制。FATF 標準將此留待各司法管轄區自行判斷，以其國家法律架構下客戶盡職審查的正式身分證明規定為準。

「可靠、獨立」的身分證據

81. 判斷如何將數位 ID 系統用於客戶識別 / 驗證的關鍵，

在於瞭解第 10 項建議規定在數位環境中「使用可靠、獨立的原始文件、資料或資訊」的要求。數位 ID 保證架構標準採用「保證」一詞來表述系統的穩健性。因此，保證等級的概念有利於判斷特定數位 ID 系統是否能「可靠、獨立」地達到防制洗錢 / 打擊資恐的目的。

82. 以下探討 FATF 現行有關「可靠、獨立」性質的規定發展過程，闡明其基本含義和目標。

83. 最初《FATF 四十項建議》（1990 年 7 月）的第 12 項建議要求受監管實體「根據正式或其他可靠的身分證明文件」來識別客戶。[22] 此用語在 1996 年 6 月和 2003 年 6 月的建議書修訂版中保持不變，直到 2012 年 2 月透過現行版本的建議書為止。2012 年，FATF 新增了「身分驗證」規定，並要求身分證明除了「可靠」之外也必須具有「獨立」性質。同時，2012 年修訂版對身分證明的類型（原始文件、數位資料或資訊）採取更靈活，更廣泛的認定方法，適用於客戶識別 / 驗證

---

22 最初《FATF 四十項建議》（1990 年 7 月）規定金融機構必須識別客戶身分，加強防範毒品販運犯罪所得的洗錢行為。第 12 建議（1990）的相關部分摘述如下（醒目標記為後加；標點符號為原文）：*金融機構不應保留匿名帳戶或明顯為假名的帳戶；此等機構必須*（根據法律、法規、監理主管機關與金融機構之協議，或金融機構之間的自律監管協議）*採用正式或其他可靠的身分證明進行身分識別，並在業務往來或交易時不時或經常記錄客戶身分*（*尤其開設帳戶或存摺、進行信託交易、租用保管箱、大量現金交易等狀況*）。

程序。該版本也刪除前版建議書對「正式身分證明文件」的明確表述。

84. 在數位 ID 的脈絡下，要求數位「原始文件、資料或資訊」必須具備「可靠、獨立」性質的意義在於：執行客戶審查所用的數位 ID 系統仰賴技術、適當治理、流程和程序，以適當確保系統得出可信的準確結果。這表示他們已經採取緩解措施，用於防範第 4 章所述風險類型。

以風險為本的客戶盡職審查方法

85. 第 10 項建議要求受監管實體使用以風險為本的方法（RBA）來確定所採用的客戶審查措施範圍，包括客戶身分識別 / 驗證。

採用以風險為本的方法來執行客戶審查措施，將有助於達成金融普惠目標

根據第 10 項建議及其註釋，受監管實體必須識別、評估並採取有效措施以減緩其洗錢 / 資恐風險（針對客戶、國家或地區；以及產品、服務、交易或交付管道）。在高風險情況下需要採取強化措施；若經確認為低風險則可能需要簡化措施。FATF 已發布相關指引，說明如司法管轄區 / 受監管實體何使用以風險為本的方法來執行客戶審查，進而支持金融普惠的發展。[23]

---

[23] FATF（2013-2017）《*防制洗錢和資恐措施以及金融普惠 - 附客戶審查增補條文*，FATF，巴黎 www.fatf-gafi.org/media/fatf/content/images/

86. 誠如第 5 章所詳述，依第 1 項和第 10 項建議及其注釋所要求，受監管實體應採用與洗錢 / 資恐風險類型和等級相稱的客戶盡職審查措施。第 1 項建議注釋強調，受監管實體在評估風險時，應先考慮所有相關風險因素，再判定總風險等級和應採取的適當緩解措施。連同第 10 項建議及其注釋，第 1 項建議的注釋特別載明：受監管實體可以根據各種風險因素的風險類型和等級來區別各種措施範圍（例如在特定情況下，一般客戶審查程序可用於客戶受理措施，而強化的客戶審查則用於持續監控，反之亦然）。

非面對面的業務往來和交易

87. FATF 會使用「**面對面**」（face-to-face）和「**非面對面**」（non-face-to-face）等術語來區分業務往來（包括客戶引導）和交易活動的類別。FATF 定義的面對面互動是由當事人在現場進行，表示互動 / 交易的各方都在同一實體位置，並透過實體互動進行活動。**非面對面的互動**則採取遠端方式進行，表示雙方不在同一實體位置，而是透過數位或其他非實體方式（例如郵件或電話）進行活動。[24]

Updated-2017-FATF-2013-Guidance.pdf

24 視國家法規而定，面對面和非面對面互動的定義可能有所不同。例如，某些司法管轄區認定視訊身分驗證屬於面對面的互動。

88. 第 10 項建議的注釋明訂「非面對面的業務往來或交易」可視為客戶審查時*潛在的*高風險*範例*。依條款規定，此聲明未要求相關主管機關和受監管實體一律將非面對面業務往來或金融交易歸類為等級較高的洗錢和資恐風險因子。相對的，此注釋是將非面對面的業務往來和交易視為洗錢或資恐風險*可能*較高的情境*範例*。

89. 有鑑於數位 ID 技術、架構、流程的進展，以及共識導向的開源數位 ID 技術標準的問世，請務必釐清下列觀念：在非面對面的客戶身分識別和交易程序中採用可靠、獨立且設有適當風減緩解措施的數位 ID 系統，可將風險控制在標準程度；而若實施更高保證等級和 / 或適當的洗錢 / 資恐風險控管措施（INR10 和 FATF 金融普惠指引所述產品功能限制及其他措施），甚至可將風險降至更低（另請參閱本指引後述「金融普惠、遠端身分證明和註冊的特殊注意事項」一節）。

現行業務往來的盡職調查

90. 此外，根據第 10 項建議（d），受監管實體必須「在業務關係中持續執行盡職調查，同時審慎檢視所有交易，藉此確保所進行的交易符合機構對客戶及其業務和風險概況（如必要，包括客戶的資金來源）的瞭解」。

91. 如前述第 2 節及附錄 A 更詳細的說明，使用數位 ID 系統進行**身分驗證**能夠確立可信度，即個人的身分已獲證實且予以核發相關憑證。鼓勵受監管實體採用數位 ID 系統驗證現有客戶的身分（作為帳戶授權流程的一環），進而利用身分驗證和相關資訊得出的資料來[25]支援現行盡職調查和交易監控作業。傳統上，相關單位是為了保護受監管實體免於遭受詐欺的而取得這類資訊。但隨著各界加速改用數位金融系統，並且逐漸依賴使用數位 ID 身分驗證機制授予帳戶存取權限，該等資訊對於防制洗錢 / 打擊資恐之目也益顯重要。

92. 對於受監管實體而言，若能在引導階段持續驗證客戶身分，將可提供合理、風險導向的保證（即可信度），以確保目前主張身分者與先前開設帳戶或其他金融服務者實為同一人，亦等同於在引導階段接受「可靠、獨立」身分識別及驗證程序的個人。現行數位化的客戶身分識別機制可用於辨識財務行為者的個人身分。因此，此機制有利於加強 R.10（d）所要求的現行盡職調查和交易監控成效。

第三方信賴要求

93. 本節說明依防制洗錢 / 打擊資恐目的而受監管之實體

---

[25] 身分驗證是帳戶存取權限授予流程的環節之一。受監管實體也可以蒐集其他補充資料（例如地理位置、IP 位址等）作為授權決策的參考。

如何能夠（1）信賴另一受監管實體採用數位 ID 進行的客戶識別 / 驗證機制（在第 17 項建議範圍內），以及（2）擔任另一受監管實體的代理人或委外實體（超出第 17 項建議範圍）。

94. 根據第 17 項建議，國家可以允許受監管實體[26] 信賴第三方執行引導階段的客戶識別 / 驗證程序，[27] 唯須滿足以下條件：

- 第三方也必須是受監管實體，應遵守第 10 項建議的客戶審查要求，且其合規性須受監管、監督或監控。
- 受監管實體應當：
  - o 立即取得有關客戶識別 / 驗證的必要資訊
  - o 採取充分步驟以達到自訂標準，確認第三方將依要求立即提供第 10（a）項建議所規定的身分識別資料及其他相關文件的副本；
  - o 確認第三方受到監管、監督或監控；根據第 10、11 項建議採取措施以達成客戶審查和記錄保存規定；以及
  - o 若第三方滿足上述條件，亦應考慮國家相關風

---

26 依第 22 項建議所述，指定之非金融事業或人員適用於 R.17 所規定的信賴關係。

27 第 17 項建議授權第三方採用第 10 項建議所規定客戶審查措施的（a）-（c）要素，但未授權使用第三方信賴功能來執行業務往來關係的現行盡職調查。本指引僅討論涉及第 10（a）項建議的識別 / 驗證規定的第 17 項建議。

險資訊，據以決定適宜的第三方所在國。

95. 如果允許這種信賴機制，則客戶盡職審查措施的最終監管責任仍歸於信賴第三方的受監管實體。

在數位 ID 脈絡下的第三方信賴機制（受監管實體也可以擔任數位 ID 服務提供者）

96. 如果司法管轄區允許，則受監管實體可以信賴其他滿足上述標準的此類實體在引導階段使用數位 ID 系統進行客戶身分識別 / 驗證，前提信賴方受監管實體可使用第三方數位 ID 系統達到下列目標：

- 立即獲得有關客戶身分的必要資訊（包括適用的保證（可信度）等級）。例如，潛在客戶可使用數位 ID 系統向信賴方受監管實體主張身分，而第三方則可以驗證該人身分並提供資訊，例如該人姓名、出生日期、國家核發之唯一身分字號，或證明在司法管轄區業務往來所需正式身分的其他屬性。
- 採取適當步驟，確認第三方將依要求立即提供第 10（a）項建議所規定的身分證據（文件、資料和其他相關資訊）的副本或適當存取方式。例如，信賴方實體可以採取適當的步驟（1）在身分證明和註冊流程中確認第三方已為受識別者建立數位 ID 帳戶，其中包含足夠的屬性證據，

以及其他身分資料和資訊；（2）第三方的身分驗證流程可依要求立即將資訊提供給信賴方。

具數位 ID 服務提供者身分的受監管實體（不屬第 17 項建議適用範圍）

97. 受監管實體若已開發自有數位 ID 系統，則可尋求成為數位 ID 服務提供者，擔任其他受監管實體的代理或委外實體。若條件允許，其服務將包括客戶引導和身分驗證流程中的客戶識別 / 驗證程序。此情況不適用第 17 項建議中的第三方信賴機制，因為第 17 項建議不涉及委外或代理關係。

98. 如同其他擔任代理或外包實體的數位 ID 服務提供者，擔任數位 ID 服務提供者的受監管實體將使用其數位 ID 系統*代表*委派方受監管實體進行客戶身分識別 / 驗證（和鑑定）。如同其他數位 ID 服務提供者，其亦可根據司法管轄區的政府稽核及認證架構尋求認證，或向信譽良好的民間認證組織尋求稽核和認證服務。

99. 無論如何，做為委託方的指定實體將繼續負責使用由數位 ID 服務提供者提供的數位 ID 系統進行*有效的*客戶身分識別 / 驗證及*有效的*鑑定，且需遵循風險基礎方法來使用數位 ID 系統進行客戶識別 / 驗證及鑑定程序，如第 5 章所述。

第 4 章：遵守防制洗錢 / 打擊資恐的數位 ID 系統的效益和風險及相關問題

100. 本章介紹數位 ID 系統對受監管實體、客戶和政府的若干潛在效益，以及需要予以識別、瞭解、監控和適當管理或減輕的潛在風險。這些利益和風險涉及防制洗錢/打擊資恐主義措施的實行，也與金融普惠有關。

101. 本章旨在促進利害關係方認識數位 ID 技術特有的潛在風險，以利採用第 5 章中所列風險基礎方法予以預防或有效管理。以下有關風險的討論無意阻卻使用可靠、獨立的數位 ID 系統，亦即達到適當保證等級（即治理安排和技術標準）且能適當應對潛在風險的系

統；亦無意暗示數位 ID 系統（尤其是用於客戶身分識別 / 驗證）較傳統記錄方法更容易受到濫用。

102. 本章亦重點介紹數位 ID 系統許多更廣泛的挑戰。通常，因應這些挑戰並不屬於防制洗錢 / 打擊資恐主管機關的直接職權範圍，但這些挑戰可能會對防制洗錢 / 打擊資恐的努力產生間接影響。

103. 本章概述特定風險和挑戰，而數位 ID 保證架構標指引提供了數位 ID 系統風險緩解措施的評估架構。司法管轄區應審查這些標準，以利解決既有的廣泛風險（涉及技術及其他相關的組織和治理），並瞭解如何減輕這些風險。

數位 ID 系統的潛在效益

加強客戶盡職審查

104. 數位 ID 系統可在金融服務中提升個人身分識別的可靠性、安全性、隱私性、便利性和效率，有益於客戶、受監管實體以及金融部門的誠信。如下所述，可靠、獨立的數位 ID 系統顯著有利於改善客戶引導期間的身分識別 / 驗證，據以鑑定身分並授予帳戶存取權限。此外，準確的客戶身分識別機制可實現他客戶盡職審查措施，包括業務往來和交易監控流程進行有效且持續的盡職調查。

盡量減少人為控制措施的弱點

105. 傳統的客戶身分識別 / 驗證記錄方法主要憑藉人為控管手段 - 例如將正式身分證明文件上的照片與開戶申人進行比對，並判斷該身分證明文件的真實性。前線人員可能缺乏可靠識別偽造、變更或遭竊文件所需的工具、技術、培訓、技能和經驗。

106. 使用可靠、獨立數位 ID 系統有助於減少人員身分識別和驗證程序發生人為疏失的可能性。

- 首先，即使在現場使用數位 ID 系統並以人工判斷的方式進行身分證明，[28] 仍通常由專家進行，可以使用先進的技術工具來偵測詐欺和遭竊的身分證件。例如，遠端身分證明（至少在較高保證等級）通常採用日益縝密和有效的數位 ID 技術，來確認身分證件是真實而非偽造，亦作為可靠的額外資料和資訊，用於證明個人身分真實無訛。[29]
- 其次，在確認客戶聲稱的身分時，數位 ID 系統

---

[28] 如第 2 章和附錄 A 所述，數位 ID 系統中的身分證明是可以在現場進行的環節（即不必在遠端運作仍可視為數位 ID 系統）。

[29] 目前，只能使用紫外線（UV）讀取或作為文件實體結構要素的安全特徵（例如安全騎縫、蝕刻或貫穿多個頁面的打孔）可能較難或無法遠端驗證，但是大多數身分證明文件都具有強大的安全功能，可以從遠端有效地予以檢查。

的身分驗證環節大致消除了主觀人為判斷的作用。具有多因素身分驗證和安全流程的數位 ID 系統，可一致可靠地判斷開設或存取帳戶的申請人與最初核發身分憑證的對象確實為同一人。

改善客戶體驗並節省成本

107. 可靠、獨立的數位 ID 系統也可以為引導階段的潛在客戶及往後要求存取帳戶的客戶提供更高效率、簡易便捷的使用體驗。客戶的接受度和便利性是完成申請、交易和客戶保留的重要驅動因素。方便客戶使用，再加上受監管實體的潛在效率提高，有助於降低客戶引導成本。一份報告指出，使用數位 ID 系統的受監管實體可將客戶引導成本降低多達 90%，身分識別 / 驗證所需時間及其他客戶審查環節從數天或數週減少到數分鐘。[30] 這些成本節約效益有助於受監管實體將合規資源分配給其他防制洗錢 / 打擊資恐的合規部門，也可以減少成本以促進金融普惠性，使原先遭排除或服務不足的客群受益。

交易監控

---

30 麥肯錫全球研究所（2019），數位身分識別，www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx。

108. 如上所述，對客戶 ID 進行可靠的數位身分驗證，以授予現行帳戶存取權限，將可促進識別並通報可疑交易，因為這有助於受監管實體判斷目前存取帳戶並從事交易者與先前存取帳戶者為同一人，且實際上即是已識別且驗證身分的帳戶所有人。此外，根據運作模式和其他因素（例如使用者同意和資料保護 / 隱私法），數位 ID 身分驗證機制不僅用於授予帳戶存取權限，亦可供受監管實體擷取其他資訊，例如地理位置、IP 位址或使用者用於從事交易的數位裝置識別資訊。這些資訊有助於受監管實體更詳細瞭解客戶行為，據以判斷金融交易的異常或可疑之處，並且輔助執法機構調查犯罪。例如，受監管實體根據資料保護和隱私規則等當地法規、透過不同方式和管道（包括網際網路和行動電話）擷取的補充資料，非常有助於判斷帳戶控制者身分他、其是否控制多個帳戶；以及使用這些帳戶進行金融交易的個人和實體網路。

普惠金融

109. 金融服務的快速數位化，大幅提升了可靠、獨立的數位 ID 系統對普惠金融的重要性，在開發中國家尤其如此，[31] 數位 ID 系統和數位金融服務已成為普惠金

---

31 在 2017 年全球 Findex 調查中，低收入國家 26% 無銀行帳戶的民眾表示乏正式身分證明文件是取得金融服務的主要障礙。

融的核心驅動力。[32] 對於無法獲得傳統正式身分文件（例如護照和駕駛執照）的金融排除者，開發靈活、結果導向的數位 ID 保證架構標準將有益於此族群以較低身分保證等級（較不嚴格的身分驗證要求）取得數位 ID，並在適當的低度風險下取得金融服務。保證架構標準亦有助於金融排除者使用替代身分證明文件（例如「可信公證人」做為具擔保效力的申請人身分證明）來獲取數位 ID。此外，數位 ID 系統適用於偏遠地區遭金融排除的族群，支援安全的非面對面身分證明 / 註冊流程，藉以進行客戶身分識別 / 驗證。這些問題將在本指引後述「普惠金融的特殊注意事項」一節中深入探討。

110. 在開發中國家，政府對個人（G2P）的支付，包括社福津貼轉帳（例如有條件的現金轉帳、子女撫育費和學生津貼）、政府薪酬和退休金的支付，以及退稅的數位化日益普遍，商務活動和零售消費者的支付也是如此。在人道主義背景下，越來越多攸關生計的援助也是以數位方式提供現金資助。所有這些活動都需要存取交易帳戶，而此程序可透過數位 ID 系統予以簡化。

---

32 FATF（2013-2017），AFATF（2013-2017）《*防制洗錢和資恐措施以及金融普惠 - 附客戶審查增補條文*，FATF，巴黎 www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html.

111. 使用可靠、獨立的數位 ID 系統，可以降低客戶審查成本，支援更多服務短缺的民眾使用受監管的金融服務（請參閱說明欄 4 的印度 Aadhaar 系統和說明欄 5 的秘魯身分識別和公民地位國家註冊局等案例）。上述發展促進了金融普惠性，並提高了防制洗錢 / 打擊資恐制度的覆蓋面和有效性。

數位 ID 系統的風險和挑戰

112. 本指引著重於客戶盡職審查特定環節所使用的數位 ID 系統用，而非傳統文件身分識別系統的用途。下述有關風險的討論無意暗示數位 ID 系統的風險高於其效益，亦未暗示其風險高於傳統的文件型身分識別系統。

113. 如同任何 ID 系統，數位 ID 系統對於身分證明、憑證和身分驗證及現行身分管理的可靠性取決於其所採用流程、技術和安全措施的強度。例如，在實體身分證和數位 ID 系統中，身分盜竊以及容易偽造或篡改的原始文件，都可能損害可靠性。特定類型的詐欺在現場或需人工介入的流程發生機率可能較低，包括較可能在遠端發生的「大規模攻擊詐騙」。雖然數位 ID 系統提供安全功能（例如安全身分驗證）而可以減輕紙本系統的特定問題，但也會增加特定風險，例如資料遺失、損壞或未經授權存取而導致的資料濫用。

114. 數位 ID 系統面臨各種技術挑戰和風險，因其通常涉及身分證明和透過開放式通訊網路（網際網路）驗證個人身分的流程。因此，數位 ID 系統採用的流程和技術在各方（IDSP、客戶和信賴方）之間形成許多網路攻擊的可趁之機。如果不仔細考慮相關的風險因素、採取適當技術保障措施、有效的治理及當責措施來解決這些問題，罪犯、洗錢者、恐怖分子和其他不良行為者可能會濫用數位 ID 系統來建立虛假身分，或刺探利用（駭入或詐騙）合法身分所綁定的驗證機制。

115. 數位 ID 保證架構標準提供一種關鍵工具，可用於識別和評估其中特定風險，並使用數位 ID 技術和流程予以緩解，並為數位 ID 的每個環節提供適當的保障。[33] 下述風險討論適用於可靠性*不足*的數位 ID 系統，其無法滿足數位 ID 保證架構標準所規定風險管理架構的需求。本章也涉及數位領域中更廣泛的連線、網路安全和隱私挑戰，可能會影響數位 ID 系統執行客戶審查的完整性或可用性。

116. 下文討論涵蓋身分證明 / 註冊及驗證等相關風險。身分證明階段的風險可能導致「假」數位 ID 的出現（藉

---

[33] 有關身分保證等級（IAL）、身分驗證保證等級（AAL）、聯合識別保證等級（FAL）用於評估和緩解這些基本階段中每個階段的風險的深入討論請參見附錄 E，以瞭解這些基本階段的風險評估和緩解方法。

由蓄意且惡意的手段騙取而得），並可用於從事非法活動。若能達到適當的身分保證等級，則可以減輕這些風險。身分證明風險與身分驗證風險兩者有所區別，後者的情況是指合法核發的數位 ID 遭到入侵，其憑證或身分驗證機制受未經授權者控制。若能達到適當的身分驗證保證等級，則可以減輕這些風險。

身分證明和註冊風險

117. 註冊流程遭到威脅的一般原因有兩種：（1）網路攻擊和安全漏洞導致真實身分遭竊（仿冒）或假造合成 ID，導致個人身分資訊（PII）遭侵害並形成虛假證據，以及（2）IDSP 或更廣泛的數位 ID 基礎設施的侵害和濫用。本節側重於第一類，因為 IDSP 的危害 / 不當行為、網路安全及廣泛的基礎架構威脅，可透過數位 ID 保證架構標準廣泛的治理 / 組織要求及傳統電腦安全控管（例如入侵保護、記錄保留、獨立性）機制較直接地予以處理，但其不屬於本指引涵蓋範圍。

冒名頂替的風險和合成 ID（涉及網路攻擊、資料保護及 / 或安全漏洞）

118. 在某方面，數位 ID 系統中的虛假證據（遭竊或偽造）

引起的實際風險遠高於前者。[34] **冒名頂替**是假冒真實個人身分的行為，可能是單純使用外貌相似者的遭竊文件，但也可能是結合偽造證明文件的虛假身分（例如使用冒名頂替者的肖像替換真實護照上的個人照片）。**合成身分**是指犯罪分子結合真實（通常藉由竊取而得）和虛假資訊假造新的（合成）身分，可以用於開設詐欺帳戶以及從事詐欺購買行為。有別於冒名頂替，這類犯罪分子偽裝的是實際上不存在的個人，而不是冒充真實存在的身分。例如，犯罪集團可能竊取身分，產生大量合成數位 ID，其部分採用真實個人的身分屬性、從線上交易或駭客入侵網路資料庫所竊取的其他資料，其餘則採用完全虛假的資訊。罪犯可能使用合成 ID 申請信用卡、線上貸款和提款，並於得逞不久後捨棄該虛假帳戶。根據數位 ID 專家說法，合成身分的使用構成了美國境內數位 ID 系統身分證明和註冊階段的最大風險。[35]

119. 為了便於說明，下表列出相關風險，並根據 NIST 指南提出若干身分證明和註冊流程威脅緩解策略。

---

[34] 上網搜尋「假 ID」可發現數以百計的網站，提供偽造駕照、護照、出生證明、移民文件及其他正式文件保證辦妥的服務，而且成品與合法版本之間難辨真偽。

[35] FATF 專案團隊與 Digital ID 專家會議，2019 年 9 月。

表 1NIST- 身分證明 / 註冊風險緩解策略

風險類型	描述	潛在的風險緩解策略
偽造的身分證明證據	申請人使用偽造的駕駛執照，宣稱不正確的身分。	IDSP（CSP）驗證所出示證據的實體安全功能。 IDSP（CSP）使用核發機構或其他授權來源來驗證身分證據中的個人詳細資訊。
詐欺性冒用他人的身分	申請人冒用他人護照	IDSP（CSP）根據從核發機構或其他授權來源獲得的資訊驗證申請人的身分證明和生物辨識。

資料來源：NIST 800-63A

驗證和身分識別生命週期管理風險

120. 特定漏洞涉及到身分驗證因素的不同的類型和數量，可能導致無法識別和意外的風險，使不肖份子向信賴方主張個人（例如客戶）的合法身分，以開設帳戶或獲得未經授權的產品、服務和資料存取權限。

121. 一些可能的漏洞範例如下（僅供參考）：

- 憑證填充（也稱為違規重播或列表清除）：網路攻擊的類型，將遭竊帳戶憑證（通常是由於資料外洩）在其他系統上進行匹配測試。如果受害者為另一個帳戶設定相同密碼（在資料外洩中遭竊），則該帳戶可能遭入侵得逞。
- 網路釣魚：一種嘗試詐欺行為，目的是使用社交詐騙攻擊（例如欺騙性電子郵件、電話、簡訊或

網站）向不知情的受害者蒐集憑證。例如，犯罪分子試圖誘騙受害者向貌似可信來源提供姓名、密碼、政府身分證號碼或憑證。

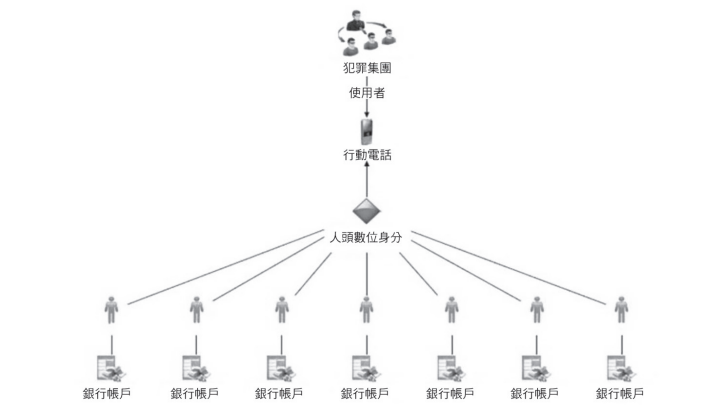
- 中間人或憑證攔截：試圖達到網路釣魚相同的目標，並且可以作為網路釣魚工具，但方式是攔截受害者與服務提供者之間的通訊。
- PIN 碼擷取和重播：方法是使用鍵盤記錄器擷取電腦鍵盤上輸入的 PIN 碼，並在使用者未察覺的情況下，趁智慧卡插入讀卡機時，使用擷取的 PIN 碼來存取服務）。

122. 大多數身分驗證漏洞是在身分所有者未察覺的情況下被利用，但也可能在訂戶或 IDSP 的知情參與之下發生濫用。例如，共用秘密身分驗證機制（例如密碼）可能會被不法分子竊取濫用，但身分憑證所有者也可能出於非法目的而故意與他人共用。

123. 例如，犯罪組織可以向個人購買數位 ID 憑證，用於存取受監管實體的個人帳戶，其實即是將它們變成組織的「數位騾子」。個人可能已經持有帳戶，或同意開設用來出售身分憑證的帳戶（請參閱下方案例研究）。

說明欄 2 人頭濫用數位 ID

瑞典的案例突顯出罪犯有系統地使用「人頭」數位 ID 來洗淨犯罪所得及由此衍生的洗錢 / 資恐風險。這是面對面交易中也可能存在的風險，但也說明了這些攻擊如何在數位世界中發生。支付服務提供者提供的即時交易服務對犯罪分子特別有利，因為它們可以與濫用的數位 ID 搭配使用，在各個帳戶之間快速轉移資金。



犯罪集團企圖濫用數位 ID 洗錢時，他們首先需要使用「人頭」的身份來開設銀行帳戶。人頭的功能是開設銀行帳戶，獲取數位 ID 和安全密碼，並將其憑證提供給犯罪集團以換取金錢。單一手機或平板電腦可以使用多個數位身分（請參見上圖）。然後，銀行帳戶就

交由犯罪集團控制。請務必注意，犯罪集團所濫用的大部分數位 ID 都是依據合法身分證據（即身分證明）而核發的。

資料來源：瑞典

124. 與防制洗錢 / 打擊資恐工作特別相關的特定身分驗證機制 / 流程的主要已知風險如下。

125. **多因素身分驗證（MFA）漏洞**：密碼是「共享秘密」的知識型驗證機制，容易受到暴力登入、網路釣魚和大量線上資料外洩等攻擊，並且很容易破解。失竊密碼、弱式密碼或預設密碼造成了 81% 的資料外洩。[36] 多因素身分驗證（MFA）解決方案，例如發簡訊到訂戶手機的 SMS 一次性代碼，為密碼 / 密碼增加了另一層安全保護，但它們也容易受到網路釣魚和其他攻擊。在至少一個因素中採用公鑰加密的防網路釣魚身分驗證機制 [37]（例如根據 PKI 憑證或 FIDO 標準建立的身分驗證機制），有助於消除這些漏洞。

---

36 Verizon 2018 資料外洩調查報告（DBIR），詳見 https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf。

37 **公共金鑰加密**機制可為一個實體（個人、系統或裝置）產生一對金鑰，由該實體安全地持有私鑰，同時將公鑰自由分配給其他實體。然後，持有公鑰的任何人都可以用它加密訊息，並放心發送給私鑰持有者，因為只有後者才能開啟此訊息。

126. **生物辨識驗證機制**：諸如指紋和虹膜掃描之類的生物實體身分驗證機制比傳統身分驗證機制更難破解，並且越來越普遍。大多數智慧型手機具有內建的指紋掃描器，某些智慧型手機具有內建的虹膜掃描器；許多個人電腦系統和高級智慧型手機中都內建臉部識別功能。

127. 罪犯者可以從中央資料庫大量竊取生物辨識資料。[38] 也可以拍攝高解析度影像（照片）、從個人觸摸過的物體採集（例如潛在的指紋）；或用高解析度影像（例如虹膜紋理）擷取，然後用於詐欺行為。然而，這類攻擊難度較高且需大量資源，因此無法擴大規模。例如，需要裝置匹配生物辨識的驗證機制無法大量被冒用，因為它們需要存取客戶的實體裝置。

128. 生物辨識技術也有許多其他弱點，會引起身分驗證的可靠性問題，並導致特定技術標準限制其身分驗證的用途（相對於身分證明）。[39] 可能無法讀取指紋或讀取不正確。不同情緒的臉部表情、臉部鬍鬚的變化、化妝以及照明條件變化，可能會使臉部識別因素變得不可靠。由於資料集不完整，臉部識別對於膚色較深和特定種族特徵的個人而言不太可靠，雖然這

---

38 在 2015 年對美國人事管理局（OPM）的攻擊中，有 560 萬套指紋影像遭竊。

39 參見 NIST 800-63-3，NIST 800-63（b）和附錄 E。

種情況正在改善。相較於基於知識或所有物的身分驗證機制，生物辨識身分驗證機制遭竊後很難註銷或替換。[40]

129. **身分識別生命週期風險**：不良的身分識別生命週期和存取管理可能會有意或無意破壞了身分驗證者的完整性，並使未授權人員可以存取和濫用客戶帳戶，進而破壞客戶身分識別 / 驗證的目的、現行盡職調查和交易監控的要求，導致無法有效保護金融系統免於濫用。

130. **未知風險**：數位 ID 系統不斷發展進化。在許多情況下，技術設計變更可改善操作效率，但只有在不肖分子展示如何刺探入侵數位 ID 系統之後，其所衍生的漏洞才會顯現出來。

在現行盡職調查和交易監控流程中存取身分資訊的潛在阻礙

131. 數位 ID 環境中的身分驗證可以促進現行客戶審查和交易監控的成效。如果受監管實體採用第三方數位 ID 系統且本身不蒐集諸如交易模式、位置、裝置存取權等資訊，則其可能無法取得分析客戶行為和交易模式所需的重要資訊，因而無法有效判定現行交易是否符合機構對於客戶、其業務和風險狀況之瞭解（必

---

40 雖然仍有方法可以註銷生物辨識憑證，但目前它們的可用性有限，而且相關的測試技術標準也仍在開發中。

要時包括資金來源）。出於反詐欺目的所蒐集之資訊，也可能有助於防制洗錢 / 打擊資恐主義的目的。受監管實體可能希望存取其帳戶存取驗證資料（或對其進行第三方分析），以偵測數位 ID 的系統濫用，包括遭駭、遭竊或出售的數位 ID。此資訊可用於識別和判斷是否通報可疑活動。聯合身分識別模式的一項重要效益是可以在身分提供者和信賴方的網路之間共用身分詐欺偵測機制。

數位 ID 系統的更廣泛問題可能影響防制洗錢 / 打擊資恐主義的成效

連線能力問題

132. 缺乏可靠的基礎架構，可能會長期破壞轄區或特定地理區域中的數位 ID 系統。但是，數位 ID 系統可以設計為支援線下和線上交易，因此無論是否存取網際網路或行動網路皆可作用。受監管實體在判斷是否使用數位 ID 系統對客戶審查時，應考慮其復原能力。

國內正式身分架構

133. 如果數位 ID 系統採用正式文件進行身分證明，身分證明文件的可靠性弱點可能會對數位 ID 系統帶來骨牌效應的風險。身分盜竊和正式身分文件的廣泛偽造，可能會破壞純文件式方法的「可靠、獨立」性質，包括缺乏防篡改或防偽造正式文件的高級安全功能，

或者在缺乏足夠身分證明的情況下核發。線上資料庫的身分竊盜對數位 ID 系統和文件記錄方法都產生類似的風險。

134. 針對有限或特定目的（與金融客戶審查無關）而開發的數位 ID，可能無法滿足其他情況的應用需求、面臨各種限制，並可能為受監管實體帶來高昂成本或無法用於客戶審查（相關範例可參見附錄 II 的說明欄 7）。

資料保護和隱私挑戰

135. 數位 ID 涉及個人資料（PII）的蒐集和處理，包括使用生物辨識技術。重要的是，數位 ID 的保證架構標準包含資料保護和隱私（DPP）要求，這些要求可能必須遵循司法管轄區及 / 或國際標準組織制定的個別標準。此外，正在開發中的技術創新解決方案（例如分散式數位身分），可使個人更有效控制 PII 與他人共享的方式，並且進一步解決隱私和資料保護問題。

136. 政府主要負責在司法管轄區內建立資料保護和隱私制度。這些要求旨在保護資料機密性；準確性和完整性，通常適用於數位 ID 服務提供者，並要求他們進行資料保護影響評估（DPIA）等方案以識別潛在挑戰並採取適當的風險控制措施。DPP 防護措施對於降低身分盜用和網路安全風險非常重要，因為這些風險可能

會破壞數位 ID 系統的可靠性。因此，根據 FATF 的第 2 項建議，防制洗錢 / 打擊資恐和 DPP 主管機關應尋求合作和協調，以確保要求和規則的相容性。

金融排除考慮因素

137. 如果數位 ID 系統不能涵蓋司法管轄區內全部或大部分人員，或是排除了特定族群，則可能會導致（或至少不能減輕）金融排除的現象，如此會構成防制洗錢 / 打擊資恐的風險。如果特定數位 ID 無法普遍適用於客戶審查，則規定使用這類 ID 也會如同無法普及於全體族群的文件 ID 一樣構成類似挑戰。無法使用數位技術或技術素養低落，都可能會使排除風險更加棘手。例如，無法使用手機或其他數位存取裝置，或缺少網路訊號及 / 或連線不穩定等因素，都可能排除貧困、農村人口或女性，以及動盪和受衝突影響地區的居民，例如難民和流離失所者。如果數位 ID 系統使用生物辨識驗證而不提供替代驗證機制，則也可能導致金融排除情形，因為特定弱勢群體生物辨識的失效率更高。體力勞動者指紋通常磨損，而導致生物辨識讀取器無法讀取。由於臉部特徵改變、脫髮或其他衰老、疾病等因素，老年人可能會頻繁發生匹配失敗；而特定種族和個體具有較深色素沉澱、眼睛形狀或臉部鬍鬚等生理特徵，導致辨識失敗比率不成比例地高。

第 5 章：採用以風險爲本的客戶盡職審查方法來評估數位 ID 系統是否充分可靠且獨立

138. 如第 3 章所述，在數位 ID 的脈絡下，要求必須使用可靠、獨立的「原始文件、資料或資訊」來識別 / 驗證客戶身分，表示數位 ID 系統應採用技術、流程、治理和其他安全措施，以提供*適當*等級的可信度。這表示數位 ID 系統應以預期的方式運作並產生準確結果，且此過程應具有適當的可信度（保證）。此外，也應該充分予以保護以免於內外部的操縱或篡改，以防透過網路攻擊或內部不法行為等手段偽造虛假身分、給予虛假憑證，或驗證未經授權的使用者。

139. 為了確定數位 ID 系統的使用是否符合第 10（a）項建議和（d）的要求，政府、金融機構和其他利益相

關方應進行以下評估：

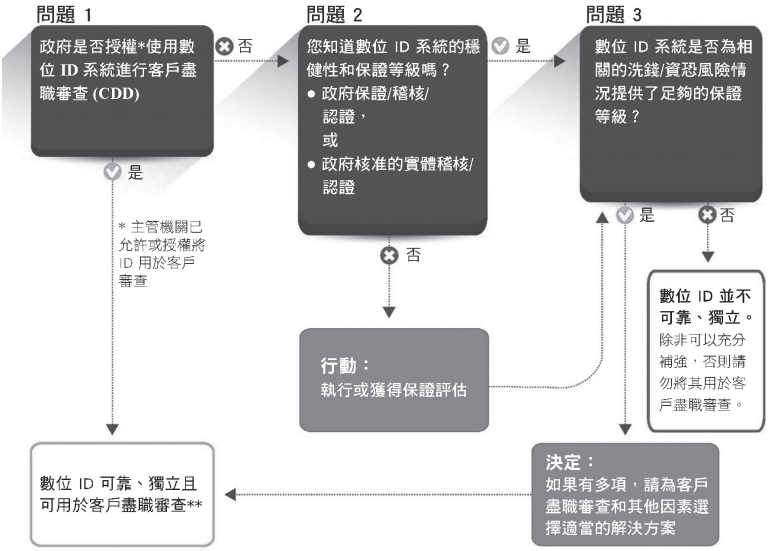
a. 瞭解數位 ID 系統根據其技術、架構和治理提供的保證等級，以確定其可靠性 / 獨立性；以及

b. 特定數位 ID 的保證等級，根據潛在的洗錢、資恐、詐欺和其他非法融資風險，使用風險方法判斷數位 ID 系統是否適當可靠，獨立。

140. 根據特定司法管轄區的數位 ID 系統和監管架構，政府和受監管實體在評估身分系統的保證等級和其對客戶審查的適用性時，可能具有不同的角色和責任，如下列受監管實體決策流程圖所示。

141. 流程圖決策流程提供一條途徑，可供受監管實體判定是否將數位 ID 系統用於客戶識別、驗證以及現行盡職調查目的。上列兩項評估分別反映在問題二和問題三中。

圖 4 受監管實體決策流程



** 在 R.10 中需要其他資訊，且可能需要其他風險緩解措施

問題一：政府是否授權數位 ID 系統用於客戶盡職審查？

142. 在問題一中，政府「支持」數位 ID 系統*並*認可其適用於客戶審查，且受監管實體可以使用數位 ID 系統，而無需執行問題二和問題三中的評估。政府實際上對受監管實體進行了建議評估中的兩項步驟（至少針對標準客戶盡職審查風險），而決策流程的其餘部分均不適用。但是，根據司法管轄區內的防制洗錢 / 打擊資恐法律和數位 ID 生態系統，受監管實體可能需要採取其他措施（請參閱下文第 147 和 148 段）。

143. 各國政府可以透過發布法規或向受監管實體提供指

導，明確地認可用於客戶審查中的數位 ID 系統，*或者允許或要求*受監管實體在客戶審查的特定部分使用數位 ID 系統。相關單位亦可能明確授權，例如政府開發並營運數位 ID 系統並建立其可信度，或設立機制來取得有關另一提供者數位 ID 系統保證等級且經過稽核及認證的資訊。

144. 各國政府也可能默許「支持」並認可數位 ID 系統適用於受監管實體的客戶審查。例如，政府可能在司法管轄區要求提供通用數位 ID 系統來證明正式身分。各國政府應對其數位 ID 系統的運作方式及其相關保證等級保持公開透明。授權用於金融部門的限定用途身分識別系統亦然。

145. 根據國內防制洗錢 / 打擊資恐法律和法規，受監管實體在特定情況下（例如風險較高時）需要補充使用授權的數位 ID 系統，並為此目的蒐集客戶審查其他方面未涵蓋的參考資訊（即瞭解業務往來的目的和預期性質）。特定司法管轄區可能設有法規，僅授權在低風險情況下使用數位 ID 系統。

146. 除了司法管轄區的法規要求，我們鼓勵受監管實體考慮是否採取其他數位 ID 風險緩解措施（如果可用），例如額外的身分屬性資料點或其他身分驗證機制及 / 或洗錢 / 資恐風險緩解措施、金融機構自有的防制洗錢打擊資恐、反詐欺和一般風險管理政策。

問題二：您知道數位 ID 系統的相關保證等級嗎？

147. 如果政府未明確或默許授權用於客戶審查的特定數位 ID 系統，則受監管實體對於其所考慮採用的數位 ID 系統，必須先確認其保證等級。[41]

148. 如果政府保證、稽核或認證數位 ID 系統（直接或授權指定組織代為決定）[42]），受監管實體可以依靠這些評估來回答決策流程中的問題二。同樣，政府也可以核准國內外的專家機構，來測試 / 稽核並認證受監管實體可能採用的數位 ID 系統。有關這些專家機構的概述請參見附錄 D。數位 ID 系統可以經認證符合最低保證等級，或者可以具有不同的、日益穩健的保證等級（統一認證的或針對各個環節），但授權資訊應公開提供。

149. 如果政府既未授權在客戶審查中使用數位 ID 系統，也未提供有關數位 ID 系統保證等級授權資訊的獲取機制，則受監管實體必須透過以下任一方式來確定系統本身的可靠性和獨立性：

---

41 如本指引前述，術語「**保證等級**」是指數位 ID 流程每個環節的可靠性或可信度等級。

42 司法管轄區的防制洗錢 / 打擊資恐主管機關可能不會展開這些行動，因為能否確定實體是否應使用適當、公開的保證架構和技術標準，可能取決於政府的另一部門。應選擇什麼權責機關來執行此職能，是每個司法管轄區需要確認的問題。舉例來說，美國總務管理局（GSA）已核准許多信任架構提供者來認證 ID 系統供政府使用。

a. 自行進行保證評估，或

b. 採納專家機構對於保證等級提出的稽核或認證資訊（雖然未經政府正式核准）。

150. 如果受監管實體自行進行保證評估，則應對數位 ID 系統提供者（包括現有的治理系統）進行適當的盡職調查，且應格外謹慎。

151. 受監管實體必須依據合理基礎得出結論，判定該實體準確應用了適當、公開的數位 ID 保證架構標準，方可採納其他專家機構的資訊。例如，該實體可由另一國政府出於類似目的予以核准，或者可由司法管轄區、地區或國際上的適當專家普遍認定為可靠無虞。

問題三：數位 ID 系統是否適合洗錢 / 資恐風險情況？

152. 如果受監管實體確實瞭解數位 ID 系統的保證等級（透過問題二所述的流程），則應分析數位 ID 系統是否足以依照 FATF 以風險為本的客戶審查方法來應對相關的非法融資風險。換言之，有鑑於客戶、產品和服務、營運地區相關的潛在洗錢 / 資恐風險，特定保證等級的數位 ID 系統是否適合於客戶識別 / 驗證及現行盡職調查？受監管實體應分析數位 ID 系統（根據其保證等級）是否足以因應相關的非法金融風險。根據司法管轄區的防制洗錢 / 打擊資恐要求及可用的數位 ID 系統，受監管實體可以選擇不同保證等級的多

個數位 ID 系統，用於進行身分證明和身分驗證。在這種情況下，受監管實體應確保系統身分證明及 / 或身分驗證的穩健性符合潛在的非法活動類型和洗錢 / 資恐風險等級。

153. 在某些國家，政府已規定（統一的）保證等級，來因應標準或較高的洗錢 / 資恐風險。受監管實體仍可以選擇所需保證等級的數位 ID 系統，或者選擇同一系統提供的不同等級身分證明及 / 或特定憑證和身分驗證機制。在這種情況下，判斷選項時應考慮其洗錢 / 資恐風險與身分證明和身分驗證的特殊關聯性。受監管實體也可以針對較低風險情境來選擇適當的數位 ID（另請參閱本節後面的有關金融普惠性的討論）。

利用數位 ID 保證架構和技術標準來實施風險基礎方法

154. 如上所述，政府（作為 IDSP 及 / 或作為監管者、監督者和政策制訂者）和受監管實體（作為信賴方）應充分考慮涉及洗錢 / 資恐風險因子和緩解防制洗錢 / 打擊資恐措施的數位 ID 風險因素和保證等級。如下文更詳細的解釋，**數位 ID 保證架構標準**對於這項評估提供了實用的工具。

155. 因此，我們建議政府和受監管實體，在評估數位 ID 系統是否滿足第 10（a）項建議的「可靠、獨立」標準時，應考慮保證架構標準所提供的資訊。此外，也鼓

勵分別考慮系統各個主要數位 ID 環節的可靠性。因為根據潛在的洗錢 / 資恐風險因素和緩解措施，對於數位 ID 系統的每個環節（身分證明 / 註冊、身分驗證或可能的聯合身分驗證）或許不需要相同的可靠性。

156. 瞭解數位 ID 系統各個環節的保證等級，有助於受監管實體採用數位 ID 來執行更縝密的、以風險為本的客戶審查方法。在金融普惠的脈絡下，**評估擔保的逐步流程方法**尤其重要。GOV.UK Verify 的技術標準和美國 NIST 800-63-3 數位 ID 指南的最終版本已為 ID 系統各個基本流程採用不同的「保證等級」。[43] 至於為整體數位 ID 系統採用單一保證等級的保證架構標準（例如 eIDAS 法規），則可以檢查流程的各個環節如何滿足每個保證等級的要求，逐一予以實施。

157. 數位 ID 技術和架構以及數位 ID 保證架構標準具動態性質且不斷發展。[44] 標準本身具有彈性，且依成果調整以促進創新。它們允許採用不的技術和架構來滿足不同保證等級的要求，並且以盡可能面向未來的方式予以建構。司法管轄區應避免採用固定的規定性方

---

43 例如根據 NIST 指南，數位 ID 流程的各個階段都有保證等級（1-3）：ID 保證等級（IAL）、驗證和憑證生命週期管理保證等級（ALA）、聯合識別保證等級（FAL）。

44 應該體認到數位 ID 標準並不總是跟得上技術發展。例如，在本指引最終定稿時，數位 ID 保證架構標準尚未解決連續驗證的問題；也沒有解決漸進身分的概念，而這項概念涉及到持續、動態的身分證明。

法，導致目前的保證等級要求被鎖定成為可靠性的上限（而非最低標準）。

使用數位 ID 保證標準和架構

158. 對於數位 ID 系統中的三項主要步驟，數位 ID 保證架構標準通常會分別設置不種等級、日益可靠的保證等級，且具有愈來愈嚴格的技術要求。

159. 正如第 10 項建議的注釋範例所述高低不等的洗錢 / 資恐潛在風險因素，技術標指引以數位 ID 系統基本流程保證等級的形式，來提供 ID *可靠性*因素。各個保證等級反映相關流程的特定等級的確實度或可信度。保證等級愈高的流程愈可靠；保證等級愈低的流程會帶來愈大的失敗風險，並且可靠性愈低。主管機關和受監管實體可以使用保證等級來評估特定數位 ID 系統的可靠性。本指引不需要或建議任何特定的保證等級。

160. 有些技術標準支援逐一評估流程的可靠性，並考量到不同的數位 ID 流程可能但未必全部處於同一保證等級（AL）。更基本的是，考慮到洗錢、資恐、詐欺和其他非法融資風險，使用風險基礎方法時必須判斷各流程適合的保證等級。即使採用單一保證等級架構，實體也可以檢查流程各個環節如何滿足各保證等級的特殊要求。

161. 為了說明相關主管機關、金融機構和其他利害關係方可在數位 ID 保證架構標準允許下用於評估數位 ID 的因素類型，***附錄 E：《美國和歐盟數位 ID 保證架構和技術標準概述》***舉例列出了美國和歐盟的保證等級。該附錄也廣義說明了身分證明的一些技術要求（數位 ID 系統的第一階段）。並且簡要註明了有關身分驗證保證等級的一些重要注意事項。

金融普惠的特殊考慮因素

數位 ID 風險管理與防制洗錢／打擊資恐風險基礎方法及洗錢／資恐風險緩解措施的關係

162. 理想情況下，採用數位 ID 系統使個人能以更高保證等級來證明正式身分，尤其在尚未為大多數人口提供可靠正式身分的國家中。但是，由於數位 ID 通常採用文件式的身分證據，因此在正式身分證系統普及率較低的國家中，由於證明身分困難，部分族群可能仍無法以較高保證等級取得數位 ID。

163. 正如本文先前所強調，面臨金融普惠性挑戰的司法管轄區應採用靈活的方法來建立所需的身分屬性、證據和證明正式身分的流程。此身分證明要求可確保金融排除族群納入身分驗證的服務範圍（例如將永久居民地址作為可選屬性，並允許受信任的個人證明其身分）。宏觀而言，在國際、政府或非政府組織針對

上述問題的因應計畫中（包括增加身分證據的取得途徑），防制洗錢 / 打擊資恐主管機關和受監管實體應考慮如何將以風險為本的客戶審查方法應用於數位 ID 系統，特別是在已知金融排除構成洗錢 / 資恐風險的司法管轄區或特定族群中。

164. 2017 年，FATF 發布了《2013 年防制洗錢 / 打擊資恐措施和金融普惠指引》增補條文，重點在於客戶審查和金融普惠性。[45] 本文重點介紹了受監管實體應配合已知風險之性質與等級所採用的風險緩解措施；並提出不同的客戶審查方法，可據以消除與驗證客戶身分有關的金融普惠性障礙，例如對可靠和獨立資訊源的廣泛瞭解，或更精簡的盡職調查措施。本指引指出，許多國家的客戶審查分層方法有助於數位金融服務的普及化。例如在這種方法下，原先遭排除或服務不足的個人帳戶將可內建防制洗錢 / 打擊資恐風險緩解措施，例如限制帳戶總額度及 / 或在指定時間範圍內交易的金額和數量，以及延遲至達到指定閾值時再驗證客戶身分。

165. 若要將 2017 年《金融普惠指引》的經驗應用於數位

---

[45] FATF（2013-2017），AFATF（2013-2017）《防制洗錢和資恐措施以及金融普惠 - 附客戶審查增補條文，FATF，巴黎 www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

ID 系統，則表示當特定潛在客戶引導過程中的洗錢 / 資恐風險較低時，可能適合採用身分證明保證等級較低的數位 ID 系統。如上所述，可能需要採取其他措施來確保降低洗錢 / 資恐風險，包括對帳戶的使用施加限制。同樣，在未經授權帳戶存取相關的非法融資風險較高（例如司法管轄區普遍存在使用者名稱和密碼遭竊的情況）但客戶相關風險較低的情況下，雖然數位 ID 系統的身分驗證保證等級較低（在客戶引導階段的身分識別 / 驗證用途），但可以對身分驗證環節提供更大的保障，以防止未經授權使用者存取該帳戶。驗證客戶的身分以授予存取帳戶和進行交易的權限，這項流程即使對於是低價值帳戶也非常重要，攸關能否有效防範詐欺性轉帳，並確保使用者無法規避各層級客戶審查的額度、速度和數量要求。

166. 在 FATF 標準下靈活使用數位 ID 系統的能力，對於金融普惠而言具有重要意義。如此可促進分層客戶審查的實施和身分驗證，因為在數位 ID 保證架構標準下，身分證明 / 註冊保證等級較低的數位 ID 系統所要求個人身分證明或驗證的嚴格性較低（請參閱附錄 E）。）。這表示，原先遭排除或服務不足的個人（缺少特定文件作為客戶引導流程所需的正式身分證明）仍可以加入數位 ID 系統。然後，該人員可以使用數位 ID 的身分驗證機制進行客戶身分識別，只要合乎指定的控管

項目和閾值，無需經過驗證即可開立帳戶。

167. 此外，數位身分識別系統可支援原先服務不足或遭排除者逐漸發展出更穩健的數位足跡和風險概況，進而能夠使用更廣泛的金融服務。取決於司法管轄區對於正式身分證明的不同規定，數位 ID 系統可能改變「正式身分」概念本身，從固定性質轉變為可隨時間推移而強化（即漸進身分）。具備漸進式身分之後，當個人（例如客戶）從事數位金融和其他線上活動並建立數位形象時，即可採用更多身分屬性和身分驗證因素，可以強化個人數位 ID，進而增加客戶身分可信度。

168. 即使在數位 ID 系統不可互通且數位 ID 不可攜權的狀況下，漸進式身分也可支持金融普惠性，因為其允許特定的受監管實體更有效瞭解個別客戶並培養業務關係的可信度，進而提供更大範圍的金融服務。然而，如果漸進式身分具有可攜權，其價值會大幅增加（包括促進金融普惠的目的），因為由單一受監管實體蒐集的個人行為模式、交易資料和相關的身分驗證資訊可建立更穩健的身分，且能隨個人行動而擺脫空間侷限，即使在不相關的受監管實體亦可用於客戶身分識別 / 驗證。如果缺乏可攜權，客戶將被迫耗費一段時間由各個受監管實體重新建立其漸進式身分，且在此期間只能存取低價值 / 低風險的產品和服務。

說明欄 3 說明分層客戶審查和逐步客戶審查中使用數位 ID 如何有利於普惠金融發展

一名金融排除者使用數位 ID 申請基本銀行帳戶，無須出具身分證明。數位 ID 的身分證明保證等級較低，但具有身分驗證保證等級，可確保聲明者掌控已知個人所綁定的身分驗證機制。

受監管實體為客戶提供服務，並提供低風險銀行帳戶，其價值、交易量和流通速度的門檻非常低，且不含跨境交易服務（這些風險緩解措施基於風險分析）。客戶可使用該帳戶來購買合約手機，用以從事各種活動，例如直接將數位薪資支付到銀行帳戶中。

受監管實體使用薪資、社會移轉或津貼相關的直接存款資料來驗證就業、職業和資金來源，並從手機和公用事業服務帳戶中定期扣款，以建立負責任的財務行為方式。受監管實體也蒐集其他交易和相關聯的身分驗證資訊來驗證客戶的地址。長期下來，受監管實體會使用客戶一致的財務活動和行為模式（例如交易時間、典型金額、目的 / 交易對手和地理位置）來加強帳戶存取和反詐欺措施的身分驗證。

司法管轄區的防制洗錢 / 打擊資恐主義法律架構是基於

原則、績效和成果而成形。其客戶識別 / 驗證法規要求受監管實體取得合理依據以掌握客戶身分，但並沒有嚴格規定他們如何實現此目標。受監管實體將特定期間內客戶活動產生的資料視為身分證據，並使用該資料來建立客戶身分及客戶風險狀況的可信度。若此可信度使監管實體確信其已履行客戶識別 / 驗證義務並滿足其自身對其他金融服務的風險胃納、風險管理慣例及程序時，該受監管實體將提供更高門檻和更大功能的標準銀行帳戶，並於之後提供小額貸款供客戶創業使用。

這種數位 ID 方法與 FATF 2017 年客戶盡職審查和普惠金融指引中規定的流程相同，其中缺乏足夠身分證件的個人可以接受分層客戶審查，並從額度有限的低風險帳戶形式開始，然後逐步擴大取得金融服務的等級。

資料來源：美國財政部

數位 ID 標準架構有助於金融普惠

「可信公證人」

169. 在一項範例中，缺乏傳統身分證明者獲准採用的數位 ID 保證架構標準就是允許可信公證人制度，例如村長、地方政府主管機關、法官 / 地方法官、雇主、社

會名譽良好者（例如商人、律師、公證人）；或其他各種經過培訓、核准或認證之個人，以根據司法管轄區的適用法律，法規或代理政策，來作為具擔保效力的申請人身分證明[46]。

170. 例如依 NIST 規定委任可信公證人要求 IDSP 執行以下操作：

- 制定書面政策和程序，規定可信公證人的決定方式（遴選標準）以及可信公證人身分的有效生命週期，包括任何限制、註銷和中止的規定；
- 依據與申請人相同的等級，對可信公證人進行身分驗證，並決定可信公證人和申請人之間確立關係所需的最低限度身分證據。

遠端身分證明和非面對面引導

171. 如前所述，數位 ID 系統可以實現遠端客戶識別 / 驗證，支援標準甚至低風險等級的遠端金融交易。技術標準允許進行遠端身分證明和註冊，即使是在更高的保證等級下也是如此。見附錄 E。

---

46 NIST 800-63A 4.4.2。IAL2 可信公證人的身分要求。

附錄 A：基本數位身分系統及其參與者之說明

本附錄以第 2 節中的簡要概述為基礎，對通用數位 ID 系統的基本環節進行了更詳細的介紹，並以概要的通論方式予以說明。本文提供若干技術或流程的範例，僅供讀者參考使用，並非鼓勵或核准使用任何特定的身分技術、架構或流程，例如生物辨識技術或行動電話技術。因此，本文適用於廣泛的數位 ID 系統。本附錄著重於數位 ID 系統的前兩個環節，因為其與第 10 項建議的應用最直接相關，亦即客戶引導階段的身分識別 / 驗證，以及帳戶存取權限所需的客戶身分驗證。此附錄目的僅為提供背景資訊，無意就防制洗錢 / 打擊資恐架構下的合格數位身分制定技術或組織要求。

數位 ID 流程摘要

正如 NIST 數位 ID 標準所反映，數位 ID 流程涉及兩項基本環節和第三項可選環節：

環節一：身分證明和註冊（含初始綁定 / 憑證）（必須）；

環節二：身分驗證和身分生命週期管理（必須）；以及

環節三：可攜權和互通性機制（非必須）。

身分證明和註冊可採用數位或書面、以及面對面（本人到場）或非面對面（遠端）的形式。[47] 在數位 ID 系統中，綁

---

47 請參閱《指引》相關術語的進一步說明。

定 / 憑證、身分驗證和可攜權 / 聯盟一律必然都是數位形式。不同司法管轄區和組織使用的術語可能略有不同，依本文所述系統而定。各階段的詳細說明如下。

環節 1：身分證明和註冊

身分證明和註冊（帶有初始綁定 / 憑證）共同構成了數位 ID 系統的第一階段。

身分證明釐清的問題是：「您是誰？」，在這項流程中，身分服務提供者（IDSP）蒐集、驗證和確認某人的相關資訊，並將其解析為特定族群或脈絡中的唯一個體。

以下討論說明身分證明處理流程的三項動作：蒐集 / 解析、（2）確認和（3）驗證。

- **（1）蒐集和解析**涉及取得屬性、蒐集屬性證據；並將身分證據和屬性解析為特定族群或脈絡中的個別唯一身分。將身分證據和屬性解析為特定族群或脈絡中個別唯一身分的流程稱為**重複資料刪除**。在某些政府提供的數位 ID 解決方案中納入重複資料刪除流程作為身分證明的一部分，可能的措施包括檢查申請人的具體履歷屬性（例如姓名、年齡和性別）；生物辨識特徵（例如指紋、虹膜掃描或臉部識別圖像）；以及政府分配屬性（例如駕駛執照及 / 或護照號碼或稅籍號碼），據以比對身分系統

中的註冊人員資料庫及其相關屬性和身分證明，以防止重複註冊。

- **證據屬性**可以是實體（文件）或純數位性質，或者是數位格式的實體屬性證據（例如紙本或塑膠駕駛執照的電子掃描檔）。傳統的身分認證採取實體形式，例如政府核發的自然人文件（為求可靠性，宜附照片、全像圖或類似保護措施），例如出生證明、國民身分證、駕駛執照或護照。同樣，傳統身分證件是由申請者親自提交給 IDSP。隨著數位技術的發展，現在可以採數位方式產生身分證件（或從實體形式轉換為數位形式）並將其儲存在電子資料庫中，進而可以比對數位資料庫，以*遠端取得*身分證據和 / 或*遠端驗證身分屬性和其他資訊*。
- 屬性也可能是固有的，即個人生物辨識特徵（可以是生物學或行為性質）。[48] 生物辨識技術的性質已從靜態單調迅速發展到動態多變，衍生出不同的種類，也帶來可靠性和隱私方面的風險。按照

---

48 請務必區別下列不同的生物辨識用途：作為身分屬性、作為身分識別或重複資料刪除的根據（即用於確立個人的身分和唯一性）以及作為身分驗證機制。數位身分技術標準（例如 NIST 標準）僅支援生物辨識技術以有限方式用於身分驗證，並針對此目的提出嚴格的要求和指引，旨在解決各種疑慮。

技術成熟度、商業採用規模以及潛在的隱私威脅的嚴重性，數位 ID 系統可能包括以下用途：

- 生物物理學生物辨識屬性，例如指紋、虹膜紋理、聲紋和臉部識別，此皆為靜態屬性。
- 生物力學生物辨識屬性（例如擊鍵力學）是個人肌肉、骨骼系統和神經系統獨特交互作用的產物，皆為動態屬性。
- 行為生物辨識屬性，是依據社會物理學門下的新分支「運算社會科學」（computational social science）得出的研究成果，包括個人各種行動和使用方式的*地理空間時態資料流*，例如個人電子郵件或簡訊格式、手機使用方式、地理位置模式和檔案存取日誌（包括預期登入管道、地理位置、時間安排、使用頻率和類型（帳戶餘額和活動審核與交易）。[49]

- 所需的（核心）正式身分屬性依司法管轄區而異，但可能包括：正式全名、出生日期、出生地、戶籍地址和政府核發的唯一身分證號碼。但是，在司法管轄區證明正式身分所需的屬性和證據方

[49] 參見 D. Shrier,T.Hardjono 及 A. Pentland《Behavioral Biometrics》第 12 章 *New Solutions for Cybersecurity*（H. Shrobe，D. Shrier 及 A. Pentland 合編（MIT Press，MIT Connection Science & Engineering，2017 年）。

面，政府的決定權頗具彈性。隨著技術發展及各種身分屬性可信度的信心持續演進，政府判定所需身分屬性的方法可能會逐漸改變。[50] 此外，政府在確立所需的身分屬性時，可能會將國家環境和金融普惠目標納入考量。例如，特別是在有大量流動人口、居無定所及無正式戶籍族群的開發中國家，政府可能決定不要求以地址作為證明正式身分的核心識別符。

- **（2）確認**是指確定證據的真實姓（不是假冒、偽造或盜用），並且對照可接受（經授權 / 可靠）的來源，檢查身分資訊 / 證據以確定資訊相符且可靠，進而判定證據包含的資訊是準確、獨立的來源資料 / 記錄。例如，IDSP 可以（1）檢查實體身分證據（身分證件），例如駕駛執照及 / 或護照，或申請人實體身分證據的數位影像，並且（a）確定沒有任何改動；證件號碼遵循標準格式；實體和數位安全功能有效且完整；（b）向政府核發來源查詢許可證及 / 或護照，並確認資訊相符。
- **（3）驗證**流程包括確認已驗證的身分可關聯到接

50 例如，隨著人機介面（HCI）技術（例如結合眼睛運動和滑鼠使用特徵）或觸控介面的發展，某些政府最終可能轉而採用生物力學屬性，來代替對於傳統識別符的依賴。有關行為生物辨識技術在數位身分識別、驗證和鑑定中的作用，相關討論請參閱第 5 章。

受身分驗證個人（申請人）。例如，IDSP 可以要求申請人拍攝並手機視訊或照片，並連同其他活體辨識證據一同發送；將申請人提交的照片與護照證件照或政府護照或許可證資料庫中存檔的照片進行比較；並確定它們是否符合特定的確定性等級。然後，為了將身分證件關聯至真實身分申請人，IDSP 可以將註冊代碼發送到與相關身分申請人經過驗證的電話號碼；要求申請人向 IDSP 提供註冊代碼；並確認提交的註冊代碼與 IDSP 發送的代碼匹配，進而驗證申請人身分真實無訛，並且擁有並控制已驗證的電話號碼。至此，申請人的身分即證明完成。

註冊是指 IDSP 將已證實身分的申請人登記（註冊）為「訂戶」並建立其身分帳戶的流程。該流程使用適當的**綁定**協定，將訂戶的唯一已驗證身分（即訂戶屬性）授權綁定到訂戶擁有和控制的一或多個身分驗證機制。將訂戶身分綁定到身分驗證機制的流程也稱為「憑證化」。

身分驗證機制是申請者擁有並控制的事物（通常是一個密碼模組、時間碼產生器或密碼），用於驗證（確認）申請者的身分。更準確地說，**身分驗證機制**是申請者擁有和控制的事物，用於驗證（確認）申請者是核發憑證的對象，亦即（取決於數位 ID 系統的驗證環節強度）是實際訂戶和帳戶持有人（依身分驗證保證等級指定不同程度的可能

性）。**憑證**是一種實體物件或數位結構，透過一或多個識別符將訂戶經證實的身分授權綁定到訂戶擁有和控制的至少一個身分驗證機制上。當數位 IDSP（擔任憑證服務提供者（CSP）核發身分驗證機制並將其可靠地綁定到訂戶身分時，其所產生的實體對象或數位結構就是身分憑證。

通常，IDSP 會向訂戶核發身分驗證機制，並在註冊時將身分驗證機制關聯至訂戶經證實的的身分，藉此註冊身分驗證機制。但是，IDSP 也可以將訂戶的帳戶綁定到訂戶提供且 IDSP 可接受的身分驗證機制（擔任 CSP）。此外，雖然綁定是可信任註冊的重要組成部分，但 IDSP 也可以在以後將訂戶的憑證綁定到其他或替代的身分驗證機制，作為身分生命週期管理的一部分，如下所述。

身分證明可以由單一或多家服務提供者提供（請參見下方數位 ID 系統參與者摘要）。在前一種情況下，單一實體、流程、技術可以執行各個身分證明流程。類似地，在註冊期間綁定證明的身分，可以由單一服務提供者或另一家並未執行身分證明的服務提供者來完成。

圖 5 身分證明和註冊

環節 2：驗證

身分驗證釐清以下問題：「**您是否為已識別 / 驗證身分的個人？**」它確定，尋求存取帳戶（或其他服務或資源）的個

人（即申請者）與下列特徵者為同一人：其身分已證實、註冊和憑證化，且擁有並控制具約束力的憑證和其他適用的身分驗證機制（例如引導客戶）。身分驗證可憑藉各種驗證因素或流程來進行，如下所述。身分驗證的可信度取決於所用身分驗證因素的類型以及身分驗證流程的安全性。[51]

驗證因素

傳統上，驗證因素分為三個基本類別：

- 知識因素：您知道的一些資訊，例如：共享機密（例如使用者名稱、密碼或密碼短語）、個人識別碼（PIN）或對預選安全性問題的答案。
- 所有權因素：您擁有的事物，例如：儲存在硬體（例如行動電話、平板電腦，電腦或 USB 加密狗）或訂戶控制軟體中的加密金鑰、硬體裝置產生的一次性密碼（OTP）；或安裝在數位裝置（例如手機）上的軟體 OTP 產生器。
- 固有因素：您的特徵（生物物理學生物辨識特徵，例如臉部識別、指紋或視網膜紋理生物特徵、生物力學生物辨識特徵、個人與數位裝置互

---

51 本指引所述身分驗證構件有別於歐盟法律架構下的「強式客戶身分驗證（SCA）」。對於 PSDII 而言，有效 SCA 因子的構成條件必須根據 SCA + CSC 上的 PSDII 和 RTS 進行評估，而不是根據 FATF 指引進行評估。

動的獨特方式，例如個人握持手機的方式、滑動螢幕、擊鍵節奏，或使用特定鍵盤或手勢的快捷方式；以及高階行為生物辨識特徵）。

如下所述，特定的數位 ID 系統未必使用這些因素中的每一種。例如，雖然目前許多數位 ID 系統都使用生物辨識技術，但不應假設所有數位 ID 系統皆是如此。

知識驗證因素（您知道的一些事物）實際上可能不是秘密。在 NIST 標準下，知識導向的身分驗證機制，亦即提示申請者回答預設只有申請者本人知道的問題，並無法構成數位身分驗證可接受的機密。同樣，生物物理學生物特徵的固有因素也不構成秘密，因此 NIST 標準僅在與實體驗證機制牢固綁定時，才允許將生物物理學生物特徵用於驗證。

重要的是，許多技術導向的所有權和固有身分驗證機制（包括進階數位裝置身分驗證機制、生物力學生物特徵和**行為生物特徵模式**）已經或正在開發和部署用於反詐欺目的，其具有顯著的潛力，可加強數位 ID 身分驗證流程，以符合防制洗錢 / 打擊資恐的要求。[52]

傳統上（且反映在 NIST 數位 ID 標準中），數位 ID 身分驗證會在特定的時間點進行：當申請者主張客戶 / 訂戶身分，並尋求進行數位（線上工作階段）或面對面互動授權，以

---

52 如本指引所述，數位 ID 系統亦存在重大風險（包括隱私風險）和遭濫用的可能性（例如偏見或侵犯人權），雖不在本指引適用範圍，但應予以有效解決。

存取客戶的帳戶或其他金融服務或資源時。但是，如今許多受監管實體（尤其是已開發國家的大型金融機構）在線上互動開始時就利用「連續驗證」解決方案來增強傳統驗證，這些解決方案利用了**生物力學生物辨識技術、行為生物辨識特徵模式**及 / 或動態**交易風險分析**。連續身分驗證並非採用申請者開始互動時擁有 / 知道 / 將要確立的組合來確認申請者是線上客戶並控制發布給該客戶的身分驗證機制 / 憑證，而是著重確保在整個線上互動流程中蒐集的某些資料點（例如地理位置、MAC 和 IP 位址、鍵入節奏和行動裝置角度）符合整個工作階段流程中的「預期內容」。

就連續身分驗證技術對於身分驗證風險的減緩效果（有效性）而言，相關的衡量方法尚未成熟，且 NID 等數位 ID 技術標準目前並不適用。第 2 項支付服務指令（PSD2）下的歐盟委員會授權法規（EU）2018/389（關於強式客戶身分驗證和安全通訊的監管技術標準）要求：所有支付服務提供者（PSP）都必須具有適當的交易監控機制，以偵測未經授權或詐欺的付款交易，藉此實施 PSD2 中的 SCA 規定（法規技術標準 [RTS] 第 2 條）。此外，如果 PSP 希望依據 RTS 第 18 條豁免於 SCA 的「交易風險分析」規定，則必須根據 RTS 第 2 條設置即時風險監控機制，並證明其詐欺率低於 RTS 定義的特定閾值。[53]

---

[53] RTS 相關條文請參見 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389。

以下討論適用於靜態、單點的時間身分驗證方法，其受到 NIST 數位 ID 標準的規範。

驗證流程

身分驗證流程通常根據所需身分驗證因素的數量和類型進行分類，其原理為：身分驗證流程採用的因素越多，身分驗證系統就可能越穩健和值得信賴。隨著身分驗證技術 / 流程的發展，此概念正透過現代化的結果導向方法進行修訂和增強，雖採用多因素身分驗證機制，但是身分驗證環節強度並不取決於所用因素及其類型的*數量*，而是身分驗證流程是否可以抵抗常見且不斷演進的攻擊（例如網路釣魚和中間人攻擊媒介）威脅。（這種更全面、結果導向的方法應可更有效因應連續驗證機制的普及化。）

依安全程度區分的身分驗證協定 / 流程類型如下：

- **單因素身分驗證（1FA）**僅使用單一身分驗證機制來驗證個人的身分。
- **多因素身分驗證（MFA）**使用至少兩種不同身分驗證因素類別（知識 / 所有權 / 固有）的兩種以上獨立身分驗證機制來驗證申請者的身分。例如，當申請者試圖使用知識導向身分驗證機制（例如使用者名稱和密碼）登入線上銀行帳戶時，申請者也需要輸入其他身分驗證因素類別的其他身分驗證因素，才能成功存取該帳戶。申請

者可以為此使用所有權驗證因素，例如手機內建的 FIDO 認證驗證器產生的私鑰。MFA 可以使用多種身分驗證機制（直接組合不同類別的身分驗證因素並提交給驗證方），也可以由單一驗證機制提供多種類型因素，例如身分驗證機制採用一或多種因素保護另一種因素，而這些因素又直接提交給驗證方。[54]

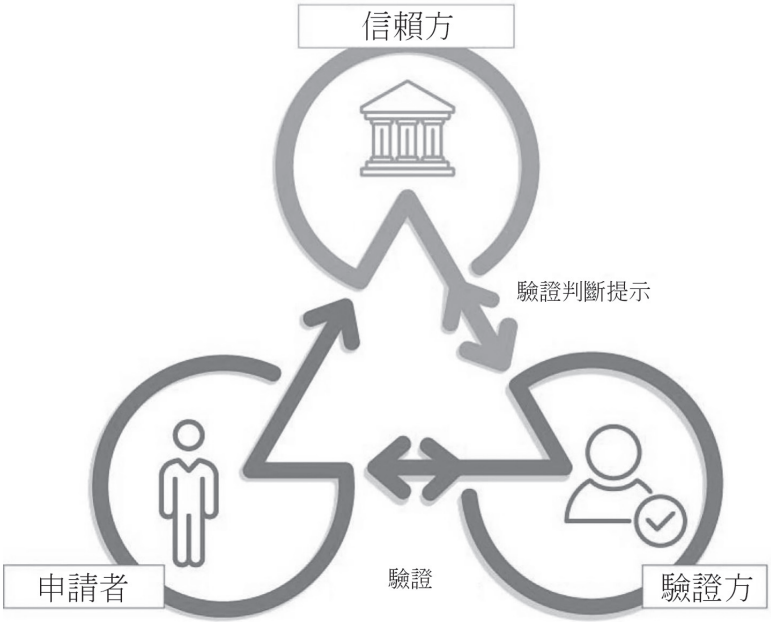
下圖以典型的金融交易為例說明驗證流程。在此圖中，一名現有客戶希望發起金融交易，首先必須透過一或多個身分驗證機制證明自稱的身分為真，即自己是帳戶所有者本人。客戶（申請者）透過安全驗證協定與 IDSP（驗證方）進行通訊，進而證明自己擁有和控制該驗證機制。驗證方透過 CSP 確認（驗證）驗證機制的有效性，並向金融機構（在示例情境中為 RP）提供驗證判斷提示。注意：CSP、驗證方和 RP 可能是同一實體（簡單兩方身分驗證，僅由申請者和 RP 組成）。

---

54 根據 NIST 標準，強式身分驗證需要雙因素身分驗證或 MFA 來執行兩種以上相互獨立且不同類型的身分驗證因素，其中至少一種不可重用、不可複製，且無法透過網際網路暗中竊取。根據 EU PSD2 規定，以及如 RTS 所重申的內容，「強式客戶身分驗證」定義為「使用兩種以上要素的身分驗證，這些彼此獨立的要素區分為知識（只有使用者知道的事物）、所有權（只有使用者擁有的事物）和固有（使用者本身的特徵）因素，因為違反其中一項不會損害另一項的可靠性，並且其設計旨在保護身分驗證資料的機密性。有關技術標準的更詳細討論請參見附錄 E。

圖 6 數位驗證

注意：CSP、驗證方和 RP 可能是同一實體（簡單兩方身分驗證，僅由申請者和 RP 組成）。



傳統上（且反映在 NIST 標準中），數位 ID 身分驗證會在特定的時間點進行：當申請者主張身分，並尋求進行數位（線上工作階段）或面對面互動授權，以存取帳戶或其他金融服務時。但是，如今許多受監管實體（尤其是已開發國家的大型金融機構）在線上互動開始時就利用「連續驗證」解決方案來增強傳統驗證，這些解決方案利用了生物力學生物辨識技術、行為生物辨識特徵模式及 / 或動態「交易風險分析」。

身分生命週期管理

身分生命週期管理是指 IDSP 為因應訂戶身分驗證機制生命週期中可能發生的事件而應採取的行動，這些事件會影響身分驗證機制的使用、安全性和可信度。這些事件可能包括：在註冊時或註冊後核發身分驗證機制並將其綁定至憑證、遺失、失竊、未經授權的複製、到期和註銷身分驗證機制及 / 或憑證。

與身分相關聯的屬性可能會每年變更。分析系統可能會發現風險訊號，顯示身分使用的方式符合詐欺或帳戶入侵的特徵（如先前在「連續身分驗證」的討論中所述）。商業身分管理系統正在建構功能，以分析身分是否及如何在其生命週期中演變。

下列討論使用功能導向術語，即 CSP 來說明特定類型身分驗證機制生命週期事件發生時應採取的因應措施，即使個別 IDSP 可能執行身分驗證機制生命週期管理以及身分證明、註冊或驗證。

- **核發和記錄憑證**：CSP 在憑證的整個生命週期中核發憑證，並在訂戶的身分帳戶中記錄並維護憑證和相關註冊資料。通常訂戶擁有憑證，但是 CSP/ 驗證程序也可能具有憑證。在所有情況下，訂戶都必須擁有一個或多個驗證機制，該驗證機制的用途（如上所述）是在與信賴方互動時主張

身分。

- **綁定（又稱憑證化或憑證核發）**：在整個數位 ID 生命週期中，CSP 也必須保留所有與各個訂戶身分帳戶關聯的身分驗證機制記錄，並且控管身分驗證嘗試動作所需的資訊。當 CSP 在註冊後將新的身分驗證機制綁定（即核發綁定憑證）至訂戶的帳戶時，應要求訂戶先以新的身分驗證機制保證等級（或更高等級）進行身分驗證。
- **身分驗證機制受損—遺失、失竊、損壞、未經授權的複製**：如果訂戶遺失 MFA 所需因素的所有身分驗證機制（或以其他方式受損），並且已完成 IAL2 或 IAL3 等級的身分證明，則該訂戶必須重複身分證明流程，以確認身分驗證申索人與先前證實的身分證據相互綁定，再由 CSP 更換遺失的驗證機制並將其綁定至訂戶的身分 / 帳戶。如果訂戶擁有 MFA 並遺失一項身分驗證機制，則 CSP 應要求申索人使用其餘的身分驗證因素進行身分驗證。
- **到期和續約**：CSP 可能會發出已過期且不可再用身分驗證的身分驗證機制。CSP 應使用與初始身分驗證機制綁定流程和協定一致的流程，在現有身分驗證機制到期之前綁定更新的身分驗證機制，然後註銷即將到期的身分驗證機制。

- **註銷（又名終止）**：當身分不復存在（例如訂戶死亡或被發現詐欺）、當訂戶提出要求或 CSP 確定訂戶不再符合其資格要求時，CSP 必須立即註銷身分驗證者的綁定關係。

環節三：可攜權和互通性機制（非必須）

數位 ID 系統可能（但未必）包括允許正式身分證明可攜權的環節。可攜式身分是指個人的數位 ID 憑證可在無關聯的公私部門實體業務往來中用於證明正式身分，而無需每次都要取得和驗證個人身分資訊（PII）並進行客戶識別 / 驗證。可攜權要求開發可互通的數位識別產品、系統和流程。可攜權 / 互通性可由不同的數位 ID 架構和協定予以支援。

聯合識別是一種允許正式身分可攜權的方法。聯合識別是指使用聯合數位架構和判斷提示協定在一組網路系統之間傳遞身分和身分驗證資訊。聯合身分架構提供了跨獨立網路的互通性，亦即提供一種可將獨立系統連結到可互通網路的基礎結構。不使用聯合識別架構和判斷提示協定的 API，是實現可攜權的另一種方法。

各司法管轄區也在開發和採用聯合識別數位 ID 架構和協定，旨在實現多種國家層級限定用途識別系統的互通性和可攜身分。

採用可信賴的聯合識別機制及其他可攜式私部門數位 ID 系統方法，可以提供許多重要效益。例如，可攜權 / 互通性有

助於信賴方（例如金融機構和政府實體）節省識別、驗證和管理客戶身分（包括用於開設帳戶和授權客戶帳戶存取）方面的時間和資源。聯盟或 API 可攜權解決方案也可以為客戶省卻為各個金融機構或政府機關提供身分證明所帶來的不便，並減少因重複暴露 PII 而造成的身分盜用風險。

例如，eIDAS 法規下的互通性架構可確保跨國合作和國家數位 ID 系統的互通性。eIDAS 架構設置的互通性基礎架構建立了以 eIDAS 節點為基礎的技術介面，而 eIDAS 節點在信賴方與節點所連接的不同國家數位 ID 方案的互連關係中扮演關鍵角色。

數位 ID 系統的參與者

如上所述，數位 ID 系統可能涉及不同的運作模式，政府和私營部門各具不同角色，分別負責開發和運作系統及 / 或提供特定的環節、子環節或流程。

下表說明基本參與者及其在通用數位 ID 系統中的角色。雖然此表格依特定功能說明各種參與者，但應瞭解：在政府提供的通用或限定用途數位 ID 系統中，是由政府直接執行（或由另一實體代表其執行）提供者 / 營運商的所有基本功能。同樣，對於私營部門數位 ID 系統，單一或多個實體可以扮演所有或特定提供者 / 營運商的角色。

表 2 數位 ID 系統的參與者

身分服務提供者	
身分服務提供者（IDSP）	這是一項通用總稱，泛指提供和操作數位 ID 系統流程和環節的各種實體。IDSP 為使用者和信賴方提供數位 ID 系統。如上所述，個別實體可以承擔一或多項 IDSP 的功能角色
身分驗證服務提供者（IVSP）	負責進行身分證明的實體（證明程序包括確認證據，以及經由驗證機制將經確認的證據連結至申請人）。
身分提供者（IDP）	這類實體負責管理訂戶的主要身分驗證憑證，並將這些憑證派生的判斷提示發佈到 RP。IDP 通常也是憑證服務提供者（CSP），但可能依賴第三方進行身分證明和憑證化流程。
憑證服務提供者（CSP）	這類實體負責向訂戶核發及 / 或註冊身分驗證機制和相應電子憑證（將身分驗證機制綁定到已驗證身分）。CSP 負責在憑證的整個生命週期中維護訂戶的身分憑證和所有相關的註冊資料，並負責向驗證方提供憑證狀態資訊。 CSP 通常也擔任註冊機構（RA）和驗證方的角色，但可以將某些註冊、身分證明和憑證 / 身分驗證方核發流程委派獨立的實體執行，稱為 RA 或 Identity Manager（IM），亦即 CSP 可以由多個獨立營運和持股的業務實體組成。 CSP 可以是獨立的第三方提供者，也可以核發憑證供自己使用（例如大型金融機構或政府實體）。除了數位 ID 服務之外，CSP 也可以提供其他服務，例如代表信賴方（RP）執行其他 CDD）/KYC 合規功能。
登記機關（RA）（或身分管理機構）	負責註冊的實體。RA 會在身分證明之後登記（註冊）申請人及其憑證和身分驗證機制。

身分服務提供者	
驗證方	這類實體會使用身分驗證協定確認申請者對一或多項身分驗證機制的擁有和控制權，藉此驗證信賴方（RP）的申請者身分。驗證方會與憑證服務提供者（CSP）互動，以確認驗證機制確實有效，並透過驗證協定向 RP 提供判斷提示。判斷提示功能會將身分驗證流程的結果以及有關訂戶的資訊傳達給 RP。為了確認申請者擁有並控制有效的驗證機制，驗證方可能也需要確認驗證機制是透過有效的憑證來連結到訂戶帳戶。驗證方負責提供一種機制，可供 RP 據以確認其與 RP 進行通訊的判斷提示完整性。驗證方的功能角色通常與 CSP、RP 或兩者結合作用。
使用者	
使用者	唯一的真實生活個體，透過數位 ID 系統進行身分證明，登記，憑證和身分驗證，並使用它來證明其（合法）身分。在數位 ID 系統中的不同階段，通常會以不同的名稱來指稱使用者，具體取決於他們在數位 ID 系統三項環節從事的活動，如下所述：
申請人	需證明身分並註冊的個人。申請人是指接受身分證明和註冊 / 綁定（憑證化）流程的人員，從申請數位 ID 並提供身分證據開始，直到身分驗證無誤、建立身分帳戶並綁定驗證機制後，申請人才成為訂戶。
訂戶（又名主體）	這類人員的身分已由憑證服務提供者（CSP）驗證並綁定到身分驗證機制（憑證），並且可以使用該身分驗證機制來證明身分。訂戶從 CSP 接收一或多項身分驗證機制和相應的憑證，並且可以使用一或多項身分驗證機制來證明身分。

使用者	
申請者	此訂戶申明自己對於信賴方（RP）身分的擁有權，並尋求使用身分驗證協定對此進行驗證。申索人是指試圖證明自己的身分以取得該身分相關權利（例如開設或存取金融帳戶）的個人。
信賴方（RP）	藉由訂戶的憑證或身分驗證機制或驗證方對申請者身分的判斷提示，透過身分驗證協定來識別訂戶身分的人（自然或法人）。RP 信任身分判斷提示的根據包括來源、建立時間、判斷提示自建立之後的效期，以及 CSP 和 RP 治理策略和流程的相應信任架構，。RP 負責驗證判斷提示的來源（即驗證方）並確認其完整性。RP 憑藉身分驗證協定的結果來確立訂戶身分或屬性的可信度，以建立業務關係（開設帳戶）或授予帳戶存取權限及 / 或進行交易。RP 可以使用訂戶的驗證身分、IAL、AAL 和 FAL 中繼資料來提供各數位 ID 環節和流程的可信度資訊及其他因素，以做出最終的身分 / 驗證或授權決策。典型的 RP 包括金融機構和政府部門。
信託架構提供者 / 信託機構	這類受信任實體負責驗證及 / 或稽核 IDSP 身分是否符合驗證和聯合識別保證等級（IAL、AAL 和 FAL）的技術標準（流程和控制）。信任架構提供者也可能負責為這些保證等級制定技術標準。信任架構提供者可以是政府實體（例如 EU/eIDAS）或受信任的產業組織，例如 Open Identity Exchange（開放身分交換組織，OIX）；FIDO（線上快速身分驗證）聯盟（針對硬體、行動裝置和生物辨識技術的身分驗證機制規範和認證，可減少對密碼的依賴並防止網路釣魚、中間人攻擊和使用遭竊密碼的重播攻擊）、Kantara 或 GSMA（用於行動通訊裝置）。

附錄 B：案例研究

說明欄 4 印度的唯一 ID（UID）編號

數位 ID 系統的功能：印度的唯一 ID（UID）編號（又稱 Aadhaar）身分計畫使用多種生物辨識和履歷資訊及有效正式身分證件，向印度所有居民提供數位 ID，無論其年齡或國籍。

印度唯一身分驗證機構（UIDAI）已發布行動應用程式 m-Aadhaar，其可產生一個「虛擬 ID」編號，與 Aadhaar 編號相關聯但有所不同，旨在提高隱私和安全性。Aadhaar 編號和虛擬 ID 均可透過 Aadhaar 資料庫線上驗證，也可以使用 QR 碼離線驗證。

金融普惠措施：UIDAI Aadhaar 註冊流程對於身分證明的要求十分彈性，以便在普遍缺乏基本身分證件的司法管轄區實現全面覆蓋，並憑藉生物辨識技術來確立唯一性。註冊必須本人親到全國各地授權註冊服務機構（主要是邦政府、中央政府機關、銀行和公部門組織）辦理，且須使用 UIDAI 依備忘錄所規定的軟體、生物特徵建檔及其他設備進行相關程序。註冊服務機構必須特殊措施來為婦女、兒童、老年人、身心障礙

者、非專技和無組織的工人、游牧部落及居無定所的一切邊緣化 / 弱勢群體註冊身分。

UIDAI 接受許多類型的身分證件，可用於在註冊時驗證核心屬性 - 共接受 32 種身分證件，其中包含姓名和照片、14 種關係證明（PoR）文件、10 種出生日期文件、45 種地址證明文件。（請參閱 https://uidai.gov.in/images/commdoc/valid_documents_list.pdf）。

如果個人沒有任何「已公告」的身分證件，而其姓名登記於戶籍文件中，且戶長已使用規定的身份證明和地址證明文件在 Aaadhar 註冊，則該個人亦可在戶長的介紹下以家庭成員的身分註冊 Aaadhar。如果沒有 PoR 或其他所需文件，居民可以委請註冊服務商或 UIDAI 地區辦公室公告的介紹人或認證人協助辦理，而他們通常會在註冊中心提供服務。

客戶審查用途：重要的是，依據最高法院 2018 年 9 月 26 日的裁決而在 2019 年 7 月透過的《Aadhaar 修正法案》因隱私理由取消《Aadhaar 原始法案》的某些規定，但基於稅捐稽徵以及收取國家統一基金出資的政府津貼、補助和服務等目的，Aadhaar 仍屬於強制法令，但不再要求開設銀行帳戶（或取得手機號碼）。相對的，

將 Aadhaar 用於客戶審查完全屬於自願性質，並且必須先取得客戶的知情同意。受監管實體可透過以下方式驗證其客戶身分：（i）Aadhaar 的身分驗證或離線驗證機制；（ii）護照；或（iii）中央政府公告的其他任何文件。

資料來源：世界銀行

說明欄 5 秘魯

秘魯的身分識別和公民地位國家註冊局（RENIEC）為眾多部門的公共和私人實體廣泛提供數位 ID 服務，以利簡化其身分驗證和鑑定流程並改善服務品質。在該國金融領域，RENIEC 是核心的客戶身分識別 / 驗證系統，負責依照秘魯電子貨幣和行動貨幣平台 Billetera Movil（BiM）的客戶審查規定來識別 / 驗證客戶身分，該系統於 2016 年 2 月啟動並提供各種服務，包括在代理機構存提款、查詢收支餘額、執行 P2P 支付以及儲值等，範圍涵蓋數百萬名客戶。

資料來源：世界銀行（2018），*數位 ID 客戶引導*

說明欄 6 奈及利亞銀行驗證碼（BVN）

每位擁有銀行帳戶的奈及利亞人民都會在銀行驗證碼（BVN）系統中註冊，該系統包括生物辨識 ID 資料庫以及由奈及利亞銀行間結算系統（NIBSS）管理的 e-KYC 基礎架構。BVN 資料庫涵蓋超過 3,600 萬名成年人，他們可以使用 BVN 號在另一家銀行開設新帳戶，開啟線上錢包或申請貸款。如此降低了引導成本，並促進金融服務市場中更蓬勃的競爭。使用 BVN 可即時進行客戶身分識別和驗證，並且允許透過行動裝置進行遠端（非面對面）驗證。NIBSS 提供了應用程式編程介面（API），允許將 BVN 整合到銀行和非銀行數位金融服務提供者，包括全國的 FinTechs。

資料來源：世界銀行

說明欄 7 墨西哥 - 將身分識別系統用於客戶審查的成本偏高

在墨西哥，*全國公民登記機構*（CURP）是基本的個人身分識別系統，雖有潛力對全國人口使用生物辨識技術，但仍缺乏唯一性的效力，且無法達到墨西哥客戶

審查法規要求的必要保證等級。

相對的，墨西哥國家選舉機構（INE）每十年發行的選民證包含兩種生物辨識形式（臉部和指紋識別），其重複風險低於CURP。INE對於墨西哥成年人的「通用」性質是根據《*一般人口法*》的一則臨時條款所確立，直到CURP達到類似於INE的保證等級之前，該法條將會是墨西哥人民的主要身分來源。

INE開發出一項服務，允許第三方根據資料庫來驗證憑證，但是該服務的必要成本正在影響墨西哥的中小型金融機構以及願意在該國設點的金融科技公司。

墨西哥在2018年頒布《金融技術法》，有鑑於當時該國ID竊盜案件頻傳，主管機關發布相關緩解措施，同時力求遵循FATF的客戶審查建議。所發布的措施包括使用INE作為受監管實體驗證憑證的主要來源，並實施使用生物辨識技術的詳細規則，促使受監管實體尋求適當的數位ID市場解決方案，以滿足客戶審查監管要求。

但是，INE的開發目的是用來當作選民證，而不是通用的身分驗證服務，因此主管機關以協調方式發起數位ID的整體改革，旨在建立一套亦可用於客戶盡職審查相關用途的正式數位ID系統。

資料來源：世界銀行

說明欄 8 聯合國難民署 – 難民的數位 ID

截至 2018 年底，UNHCR（聯合國難民署）估計全球有 2,590 萬名難民和 350 萬名尋求庇護者。已開發國家收容 16% 的難民，而全球難民人口的三分之一（670 萬人）位於全球開發程度最低的國家。

東道國主要負責向難民核發正式身分證明，然而此程序可能交由國際認可和授權的機構來管理。

難民身分在許多方面都遭遇了獨特的挑戰。許多難民到達東道國時沒有身分證明，因為這些憑證逃難過程中被遺棄、遺失或毀損。有些難民可能未曾取得正式身分證或其他證件，通常是因為來自動盪或受衝突影響地區，或遭受歧視而無法註冊。另一方面，一般的通則是禁止在未經難民同意及有任何傷害風險的情況下與原籍國的主管機關聯繫核實難民身分。因此在國際標準下，難民身分證明更需要藉助在本人申請和面談期間蒐集的證據，以及對申請人原籍國、當地文化和其他當地資訊的瞭解。透過長期的定期接觸、確認以監控一致性、緩解風險並使難民在新環境建立身分，將可提高身分保證等級。

許多東道國政府和 UNHCR 使用 UNHCR 的數位 ID 系

統，來登記並管理尋求庇護者和難民的身分。到 2020 年 3 月，已對 72 個國家 900 萬以上的難民進行了生物識別登記。

數位 ID 系統的特點：

- UNHCR 正在強化尋求庇護者和難民的數位 ID 系統。UNHCR《註冊和身分管理指引》[55] 第 5.3 節「確定個人身分：文件審查和資料蒐集」和第 5.6 節「生物特徵識別登記和照片」說明了這類個人的身分證明和註冊流程。
- UNHCR 的數位 ID 系統提供的身分驗證方式因國家背景和使用案例而異。該系統發布的身分憑證主要用於面對面環境。尋求庇護者和難民的身分憑證均根據所在國政府的要求而有所不同，但皆包含臉部影像和履歷資訊，最低限度的資料集和其他可識別個人的唯一屬性。身分憑證也具有印刷條碼或 QR 碼，以及持有人的唯一參考號。
- UNHCR 的數位 ID 系統支援採用生物辨識技術的身分驗證，其最初用於分配人道援助物資，包括現金轉帳（稱為現金介入）。例如，

55 UNHCR，「註冊和身分管理指引」https://www.unhcr.org/registration-guidancechapter5/registration/

在包括約旦在內的中東許多國家中，發放現金的介入措施是透過內建虹膜掃描設備的 ATM 來驗證使用者的身分。

- 在馬來西亞和印尼，主管機關使用 Android 應用程式來檢查 UNHCR 發放給難民的身分證件有效性，並與應用程式中顯示的照片進行比對，更方便驗證持有人的身分。
- 烏干達的總理公署（負責難民登記和身分識別，並使用 UNHCR 的數位身分識別系統）與烏干達通訊委員會及 UNHCR 合作開發一套系統，允許 SIM 卡提供者在銷售點進行生物辨識身分驗證。撰寫本文時，該流程仍在測試中。索馬利亞政府設立了生物特徵驗證機制，以便為返國的難民提供金融服務（更多資訊請參見下文）。

數位 ID 系統的參與者：參與者在 UNHCR 數位 ID 系統中的作用因國家而異。

- 如果 UNHCR 代表東道國政府，或基於難民返國和重新安置之目的而登記和管理難民身分，則 UNHCR 是唯一的資料控制方。

- 其他情況採用了混合解決方案 - 最常見的情況是所在國使用 UNHCR 的系統來登記和管理難民身分。在這種情況下，UNHCR 提供系統，東道國政府和 UNHCR 是聯合資料控制者，受資料共享協定的規範。
- 就埃及、伊拉克、約旦、黎巴嫩和敘利亞使用的生物辨識系統而言，UNHCR 在資料保護協定的範圍內與私營部門提供者合作。

客戶審查和相關法規用途：允許 UNHCR 的數位 ID 系統及由其核發的憑證用於各個國家客戶引導階段的身分識別 / 驗證，包括：蒲隆地、馬拉威、約旦、尼日和尚比亞。[56]

索馬利亞央行已同意採用特定客戶審查方法來處理難民返國事宜，這些難民已在肯亞及其他鄰國的 UNHCR 系統中註冊生物辨識特徵。難民在離開庇護國之前填寫自願 UNHCR 核發的自願返國表格，並使用 UNHCR 系統進行生物特徵身分驗證，以便識別 / 驗證客戶身分以開設銀行帳戶。該解決方案於 2018 年 12 月進行了測試，當時為兩人開設了帳戶，並有望在 2020 年與金融服務供應方合作在更大範圍內實施。

---

56 UNHCR，「居無定所和失聯族群」（Displaced and Disconnected）（2019）https://www.unhcr.org/innovation/displaced-and-disconnected/

系統的保證等級：尚未根據本指引所述數位 ID 信任架構和技術標準對 UNHCR 系統的保證等級進行稽核，但是在撰寫本文時，UNHCR 已委託專家顧問進行外部鑑定，目前正在評估結論。

金融普惠性：經濟包容是讓難民獲得保護、自力更生和培養復原力的重要條件。自 2016-19 年以來，UNHCR 共核撥 24 億美元用於人道現金介入措施。為了促進金融普惠性，UNHCR 受益人的銀行或行動貨幣帳戶（依當地法規）提供現金介入措施，並優先考慮利用本地市場和生態系統的「開放式」系統，而不是投資於「封閉式」系統循環，後者對金融普惠性的貢獻有限。UNHCR 特別利用數位技術和行動平台，旨在促進金融普惠性，對難民的生活產生了積極而明顯的影響。

資料來源：UNHCR

說明欄 9 中國 - 私營部門提供的數位 ID

數位 ID 系統的功能和參與者：螞蟻金服依據客戶審查資訊建立一套數位 ID 系統，相關資訊均已透過中國公安部（MPS）的驗證，並蒐集了包括臉部識別在內的其他資料。客戶的姓名和 ID 號碼由 MPS 的授權資料

庫進行驗證，以確保身分資訊的準確性。人臉識別（與有效文件上的頭像匹配）、多管道交叉驗證、黑名單篩選等因素配合業務情境的考量，據以完成客戶的盡職調查。每次驗證均需要使用者明確授權並確認使用驗證服務。

金融服務用途：螞蟻金服與金融機構合作，為客戶提供保險、基金、小額信貸等金融服務，並充分利用數位 ID 向金融機構提供客戶身分識別、客戶風險評估等服務。螞蟻金服的數位 ID 已廣泛應用於各種金融服務情境，為數億支付寶使用者提供了超過 30 億個臉部驗證服務。此系統也用於年金查詢、徵收，納稅申報和其他公共服務。此外，螞蟻金服為沒有中國銀行帳戶但希望使用行動支付的短期遊客提供數位 ID。螞蟻金服向移民局採取了特殊的身分驗證措施，以確認護照資訊的真實性。

系統的保證等級：中國沒有公開透明的數位 ID 保證架構和技術標準，但若按照 NIST 標準進行評估，據稱螞蟻金服數位 ID 系統可能具有身分保證等級 2（IAL2）、身分驗證保證等級 1（AAL1）和聯合識別保證等級 2（FAL2）。

金融普惠措施：

對於無法存取銀行帳戶的農村、偏遠欠發達地區的居

民、無法使用攝影技術支援臉部識別的居民而言，螞蟻金服可以透過公民身分資訊驗證平台來驗證客戶資訊。設有帳戶額度限制（付款不能超過 1000 元人民幣），並且不允許跨境付款。

對於無法存取銀行帳戶的大學生，螞蟻金服可以透過「中國高等教育學生信息網」來驗證學生身分，包括學歷。

來源：中國

說明欄 10 新加坡 – 國家數位身分（NDI）

在國家數位身分（NDI）制度下，新加坡政府開發數位身分服務堆疊，以供新加坡居民和企業便利、安全地與公私部門進行數位交易。NDI 採用公開金鑰基礎架構（PKI）密碼安全技術，該服務自 2017 年以來已逐步部署，並有望在 2020 年全面上路。

數位 ID 系統的功能：NDI 堆疊中有 4 個不同的層。

- 受信任的資料：MyInfo 構成了 NDI 的受信任身分資料服務，於 2017 年初啟動。MyInfo 包含從各個政府機構取得經過政府驗證的資料，並包含 100 多筆個人資料項。此系統為公民和

居民提供了存取及控管資料共用行為的權限。公眾可以在個人同意的情況下，透過可靠且獨立的管道，在公私部門電子服務系統中自動填入政府驗證的個人資訊。

- 受信任的身分：政府將建立一個國家憑證核發機構（NCA），向每個居民核發以安全方式產生並內存於手機中的密碼式數位身分。政府和民間企業都可以普遍信任此數位身分。此系統將支援多層身分保證模式，允許使用者隨身分保證等級提高，進行更敏感的交易。
- 受信任的存取：NDI 將可支援身分驗證服務提供者（ASP）的開放式聯合生態系統。政府將營運其中一個 ASP，但是其他 ASP 可以由民間部門營運，而兩者均以政府核發的相同數位身分為準。SingPass Mobile 在 2018 底推出一項功能，無需硬體權杖或 SMS-OTP 即可實現安全身分驗證，進而提供更大的數位包容性並簡化了公私部門的存取程序。
- 受信任的服務：建立在 NDI 層上的數位服務。其中一個例子是數位簽章。金融機構可以憑藉 NDI 提供更受信任和高度保證的服務，並簡化客戶歷程，而不受系統或組織的邊界限制。

數位 ID 系統的參與者：受信任的資料和受信任的身分層由政府提供。受信任的存取層將用於支援身分驗證和數位簽章服務提供者（ASP 和 DSAP）的開放式聯合生態系統。政府將會營運其中一個 ASP。

客戶審查用途：如今，新加坡有 60 多家金融機構利用 MyInfo 的 220 多種數位服務進行客戶引導和執行客戶審查。

數位 ID 專屬的相關防制洗錢 / 打擊資恐法規：新加坡金融管理局發布的相關法規稱為《非面對面業務關係使用 MyInfo 和客戶盡職審查措施之指引》（AMLD 01/2018）。[57] 在使用 MyInfo 的情況下，金融機構不需取得實際文件來驗證客戶身分，也不必分別取得客戶照片。MAS 明確表示認定 MyInfo 能可靠且獨立地驗證客戶的姓名、唯一識別號碼、出生日期、國籍和居住地址。金融機構必須按照新加坡的監管要求，維護適當的資料記錄，包括從 MyInfo 獲得的資料。

系統的保證等級：NDI 已使用 USNIST 和 EU e-IDAS 作為參考範例。隨著新加坡展開雙邊合作，NDI 將根

57 www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Circular-on-MyInfo-and-CDD-on-NFTF-business-relations.pdf

據其他國家的保證等級評估其保證等級。在身分驗證方面，其採用的是 AVA 通用標準（CC）來評估保證等級（EAL）：弱點評估（AVA_VAN，從 1 到 5）級。

金融普惠性：NDI 免費提供給所有新加坡公民和居民使用，並且列為相關政府機構參與計畫的一部分。

資料來源：新加坡

說明欄 11 南非

為了減少詐欺和身分盜竊，以及滿足客戶審查日益成長的需求，南非銀行風險資訊中心（SABRIC）於 2002 年成立。SABRIC 最初由四家最大的銀行組成，目前也包括其他銀行、三家現金轉帳和一家 ATM 服務提供者。2007 年，SABRIC 與內政部（DHA）開始合作打擊與身分相關的犯罪。最初，銀行會檢查附有條碼的綠色 ID 簿外觀，並將內頁照片用來目測比對（潛在）客戶的外貌，藉此驗證客戶身分。但是，這種「人工」身分驗證方法存在弱點。為解決這些問題，SABRIC 成員與 DHA 合作，直接將其指紋與 DHA 的生物辨識 HANIS 資料庫進行匹配，而該資料庫會回傳「已驗證」或「未驗證」的回應，藉此方法驗證客戶的身分。南

非國家資訊技術局（SITA）在參與計畫的銀行設置了用於存取 DHA 資料庫的安全連線。銀行向 DHA 支付驗證費用。驗證流程會產生稽核追蹤資訊，而系統則提供了可靠的管理資訊。截至 2018 年底，有 7 家銀行和 4,000 家分支機構參與了此專案。目前，每月的驗證次數約為 300 萬。DHA 資料庫的查詢通常持續 4 到 16 秒。2% 到 3.8% 的電子驗證都沒有成功，因為接受身分驗證的個人缺乏 HANIS 的生物辨識記錄。

資源：世界銀行

說明欄 12.eIDAS 的互通性和相互承認

在 eIDAS 架構下，成員國可以使用數位 ID 來存取線上服務。他們也可以決定讓私部門參與提供數位 ID 解決方案（方法）。根據相互承認的原則，如果成員國允許使用數位 ID 在線上存取公共服務，則成員國之間有義務接受彼此公告的數位 ID 方法，且該公告方法的保證等級必須高於或等於存取服務所需的保證等級。eIDAS 法規定義三種不同的保證等級（低度、實質和高度），具體取決於所聲稱或主張個人身分的可信度。

資料來源：歐盟執委會

說明欄 13 比利時 –eCard 和 ItsMe®

比利時的數位 ID 系統涵蓋公私部門。政府會提供通用的數位身分憑證，即比利時公民 eCard 和外籍人士 eCard（合稱比利時 eCard），詳如下文所述。此系統也提供了電子政務服務專用的數位身分驗證平台。幾乎所有比利時公民和居民都擁有 eCard，目前可存取 800 多種電子政務應用程式，包括網上稅收、社會保險和電子衛生保健應用程式、網上警政、地區政府的應用程式以及線上市政入口網站。此外，私營部門數位身分驗證服務 itsme® 提供行動電話身分驗證機制，這些身分連結到 eCard 以及參與銀行和行動網路營運商（MNO）方案的特定行動電話和 SIM 卡。現有客戶可以使用 Itsme® 驗證其身分，以便登入其帳戶並進行交易。

<u>數位 ID 系統的特點和主要參與者：</u>

eCard

- 比利時電子卡的註冊需要親自進行。市政府 / 領事館和大使館負責 eCard 的身分證明、註冊、核發和交付。
- 比利時政府提供聯合識別身分驗證服務（FAS），來針對政府服務的線上存取活動進

行身分驗證。FAS 平台支援網路瀏覽器和手機存取，並採用 IETFTLS 標準，可透過網路提供端到端密碼通訊安全性。FAS 身分驗證步驟如下：

- o 公民或外籍人士在線上輸入個人 eCard 的 PIN 碼以要求登入電子政務服務。
- o 網路瀏覽器會向 FAS 發送一個身分驗證憑證，其可能是必要的憑證驗證因素，用以確保所呈現的 TLS 客戶端身分驗證憑證的完整性、有效性和真實性。
- o FAS 對憑證進行身分驗證，使個人可以完成登入並存取其所請求的政府應用程式。

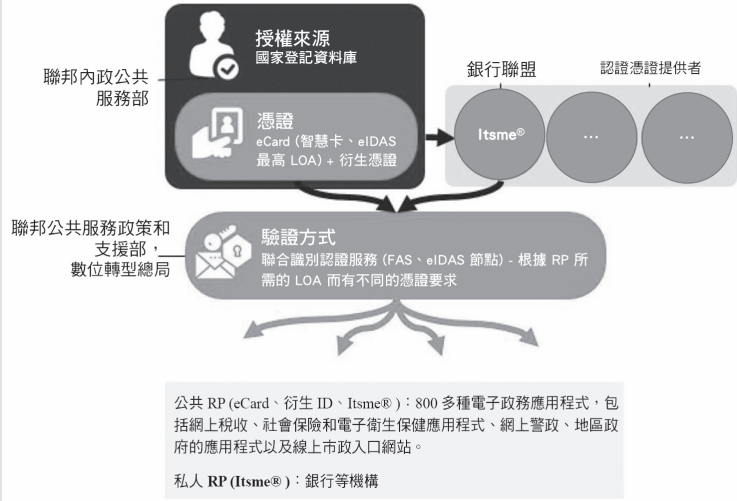
Itsme®

- Itsme® 是比利時行動 ID 的一項倡議計畫，由四家領先的比利時銀行（Belfius、BNP Paribas Fortis、ING、KBC）和行動網路營運商（Orange、Proximus、Telenet）組成的聯盟。行動裝置的 Itsme® 需綁定比利時 eID 卡方可啟用，旨在確保身分證明的效力。使用 itsme® 應用程式來進行 itsme® 使用者與 FAS 之間的身分驗證流程採用了 OpenID Connect 標準（文件參考號為 1.2.4）。

在金融服務中的用途：比利時 FAS 平台僅可用於存取公共服務，目前無法使用金融服務。itsme® 解決方案用於驗證交易。

系統的保證等級：

- 比利時 eCard 具有高等級的保證效力，這是經由 eIDAS 合作網路確認和成員國進行深度同儕審查得出的結論。
- Itsme® 已透過全面的安全和治理稽核，並獲比利時政府認可為具有「高度」保證等級的有效驗證方法。



1 使用 ECard /讀卡機首次登入 FAS 後，可以請求其他衍生的身分驗證機制（透過行動應用程式進行 OTP 驗證，或使用保證等級要求較低的應用程式輸入文字、權仗、使用者名稱/密碼）

資料來源：比利時

說明欄 14 瑞典 –eID 架構和 BankID

瑞典政府設有一個管理瑞典公民和居民身分的中央資料庫，並透過公私合作關係促進數位 ID 的便利度。政府提供聯合數位 ID 架構（eID 架構 - 瑞典連線技術架構），由包括銀行在內的私人實體擔任數位 ID 服務提供者，負責核發數位 ID 憑證並提供身分驗證服務。

數位 ID 系統的特點和主要參與者：此聯合架構既包括數位 ID 服務提供者，也包括在線上提供商品、服務或政府服務的信賴方。目前有四家數位 ID 服務提供者：（1）AB Svenska Pass、（2）BankID、（3）Freja eID 和（4）Telia E- identification，雖然 Telia 在 2017 年秋季停止受理個人註冊電子身分，但其核發的電子身分憑證仍有效至到期為止。

BankID 於 2003 年首次推出，由 10 家瑞典銀行組成的聯盟管理，為客戶提供免費的數位 ID，用於公私部門之間交易的身分驗證。企業紛紛尋求整合 BankID，方法是與 BankID 網絡成員銀行簽訂服務合約，並支付 BankID 服務費用，如此可為參與的銀行創造營收來源。身分憑證具有「硬式」（編碼在智慧晶片）或「軟式」型態，後者可以是使用者的個人電腦、平板電腦、手

機或其他數位裝置上的軟體。

在金融服務中的用途：銀行 ID 可用於引導客戶。首先要獲得銀行 ID，個人必須接受數位 ID 核發銀行的文件型客戶盡職審查。取得銀行 ID 後，即可用來在其他金融機構開設帳戶。截至 2016 年，BankID 每年促成 20 億筆交易，超過 80% 的瑞典公民都在使用它。

數位 ID 專屬的相關防制洗錢 / 打擊資恐法規：《防制洗錢 / 打擊資恐法》明確規定使用數位 ID 進行客戶身分識別 / 驗證（第 3 章第 7 節）：

「責任實體應依據身分證件、登記資料庫摘錄資訊，或透過其他資訊和獨立可靠來源的文件來識別並驗證客戶身分。

在第 1 子節的應用中，可以使用符合 eIDAS 法規的電子身分識別和受信任的服務工具。亦可使用其他經相關機構監管、認可、核准或接受的安全之遠端或電子身分識別流程。」

系統的保證等級：瑞典電子身分認證委員會根據 Svensk 電子法規來對電子身分核發機構進行查驗。瑞典 eID 保證架構定義了四個保證等級（1 到 4）。[58]

資料來源：瑞典

[58] https://docs.swedenconnect.se/technical-framework/mirror/digg/Tillitsramverk-for-Svensk-e-legitimation-2018-158.pdf（瑞典語）

參考資料：

https://elegitimation.se/inenglish/howeidentificationworks.4.769a0b711614b669f2953f.html

說明欄 15 義大利 - 數位 ID 公共系統

數位 ID 系統的功能和參與者：義大利數位身分公共系統（SPID）是根據歐盟 eIDAS 法規開發並於 2016 年啟用的公開數位 ID 系統，允許任何獲得義大利數位化機構（AgID）認可的公共和私人實體（身分提供者）向 18 歲以上的自然人（公民及 / 或具有居留證的個人）提供數位身分註冊服務，並驗證 SPID 數位 ID 憑證，進而使受識別個人能夠存取公共和私人服務。截至 2018 年 3 月，SPID 擁有約 250 萬個數位身分。SPID 註冊可在現場或線上進行，也可以使用帶有網路攝影機的行動裝置進行註冊，具體取決於特定身分提供者的註冊程序。若要取得 SPIDID 憑證，個人可以向身分提供者出具有效的身分證件（身分證或護照）、健保卡、電子郵件地址和手機號碼，或使用數位簽章、電子身分證（CIE）或國家服務卡（CNS）。

在金融服務中的用途：公共部門依法必須接受 SPID，

其在私營部門（商業和金融）則屬於非強迫性質。根據 ABI 實驗室（義大利金融協會）對義大利銀行的調查，到 2019 年底有 38% 的範例銀行預定將 SPID 系統用於引導行動銀行客戶，而 18% 的銀行預定將 SPID 系統用於網路銀行。

數位 ID 專屬的相關防制洗錢 / 打擊資恐法規：義大利法律允許有義務的實體使用符合 eIDAS 的數位 ID（例如 SPID）來識別和驗證自然人客戶的身分。

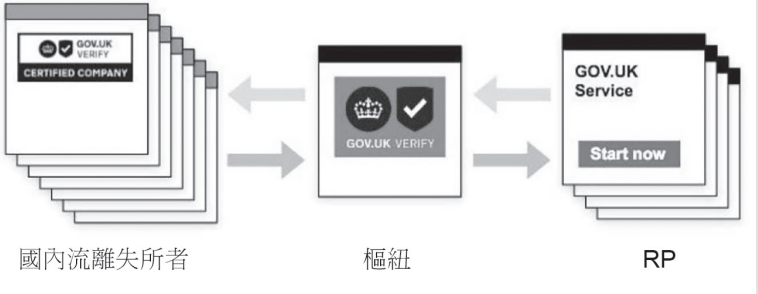
系統的保證等級：SPID 提供三種身分驗證保證等級，與標準 ISO-IEC29115 一致。等級 1 允許透過使用者選擇的名稱和密碼存取線上服務。等級 2（對於需要更高安全性的服務）允許透過使用者選擇的使用名稱和密碼加以存取，並產生可透過數位裝置（例如智慧型手機）使用的臨時存取代碼（一次性密碼）。等級 3 提供其他安全措施，包括使用由身分管理商提供的實體裝置（例如智慧卡）。SPID 身分驗證所需的保證等級取決於線上服務提供者所需的安全等級。

資料來源：世界銀行、義大利銀行和歐洲銀行聯合會

說明欄 16 英國 –GOV.UK 驗證

2012 年，英國政府發布了政府數位化策略，推出「數位首選服務」的概念 - 即線上提供服務，並允許有相關需要的使用者獲得廣泛存取權限，而不排除任何無法或無意願透過線上存取服務的族群。在「預設首選服務」政策中，人們認知到需要一種強大的數位 ID 解決方案以供使用者能在線上證明身分，並讓政府信任這些使用者自稱的身分。

GOV.UK Verify 是一套聯合識別數位 ID 系統，專供英國公民和英國居民在線上證明自己的身分。此系統使用私營部門的身分提供者（IDP）進行身分證明，並根據一組特定的要求和規範來驗證個人身分。IDP 已達到政府和產業標準，足以提供 GOV.UK Verify 系統中的身分保證服務。



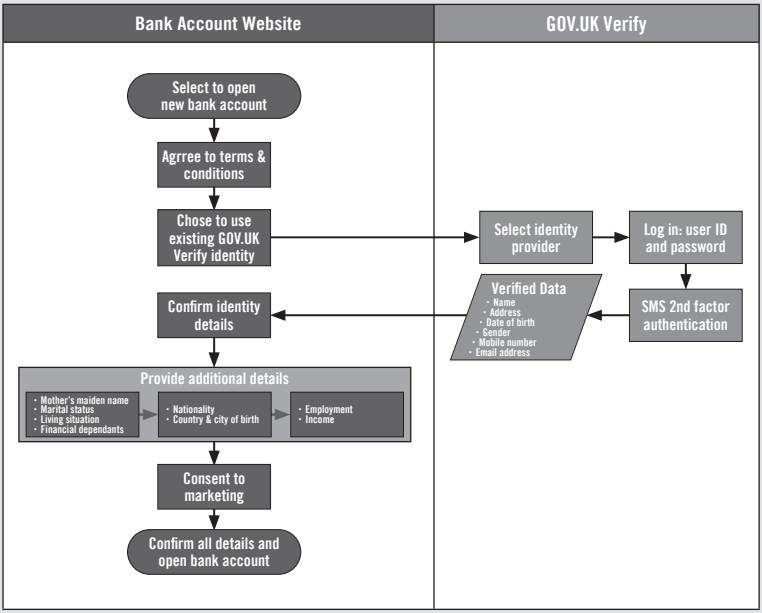
GOV.UK 驗證中心是集中化供應的基礎結構，用來管

理使用者、政府服務、IDP 和匹配服務之間的互動，只在驗證政府服務使用者的身分，並且確保 IDP 請求所需的身分保證等級。

稱為「文件檢查服務」（DCS）的產品是一項 API 端點，可讓 IDP 根據政府資料庫來查驗英國政府核發的文件，以支援 GOV.UK Verify 的身分證明作業。

GOV.UK Verify 的所有帳戶都必須至少達到 2FA。

由 Open Identity Exchange 開發的下圖顯示了使用 GOV.UK 驗證開設銀行帳戶的原型流程。



資料來源：OIX（2017），https://openidentityexchange.org/

wp-content/uploads/2017/01/The-value-of-digital-identity-to-the-financial-service-sector-Full.pdf p.13

資料來源：英國

說明欄 17 愛沙尼亞

數位 ID 系統的功能：愛沙尼亞有一系列數位 ID 系統，包括：

- 身分證 - 愛沙尼亞的主要身分證件，對所有公民和居民都是強制規定，並且是使用最廣泛的數位 ID 選項。身分證上有一張照片和一塊晶片，該晶片使用公鑰基礎架構（PKI）安全地儲存個人身分資料和數位簽章憑證。
- Mobile-ID 是私有部門的數位 ID 服務，可以透過個人手機使用。Mobile-ID 是由電信提供者根據個人的 SIM 卡和 ID 卡予以核發。該服務需要在警察和邊防局（PPA）的網站上啟用。
- Smart-ID 是私營部門的數位 ID 服務，在個人手機和 Smart-ID 金鑰管理伺服器的服務上使

用 Smart-ID API。Smart-ID 可以核發給具有愛沙尼亞個人識別碼的人士。在識別和驗證客戶方面，其功能類似於 ID 卡和 Mobile-ID。

數位 ID 系統的參與者：

- 愛沙尼亞資訊系統管理局（RIA）協調數位 ID 驗證解決方案。警察和邊防委員會根據《身分證件法》核發身分憑證（身分證、居留卡 Digi-ID、和電子居民系統的 Digi-ID）。外交部負責管理電子居留計畫。
- 兩家私營公司提供技術解決方案 -Tieto Estonia AS 為 ID 卡的基本軟體提供支援，而 SK ID Solutions AS 負責核發並確認 eID 憑證。

客戶盡職審查用途：愛沙尼亞數位 ID 解決方案可用在客戶引導階段的身分識別 / 驗證，以及符合指令（EU）2015/2366（第二項「支付服務指令」）及其監管技術標準的強式客戶身分驗證，據以授權付款交易。

數位 ID 專屬的相關防制洗錢 / 打擊資恐法規：在愛沙尼亞，客戶可透過資訊技術方法（視訊註冊）並使用兩種不同的身分驗證來源，以面對面的方式註冊。法令對此兩種驗證方法並無強制規定，但愛沙尼亞金融

監督局已發布了相關指引[59]，表示數位 ID 解決方案（即透過數位 ID 驗證取得的資訊）可以是這些來源之一（第 4.3.1.22 點），但應有額外資訊源（第 4.3.1.23 點）用於驗證客戶的身分。

系統的保證等級：在 eIDAS 方案下，所有已公告的愛沙尼亞 eID 方案都具有較高的保證等級

資料來源：愛沙尼亞

59 www.fi.ee/sites/default/files/2019-01/FI%20rahapesu%20t%C3%B5kestamise%20juhend%202018%20%28EN%29_pdf.pdf

附錄 C：永續發展的身分識別原則

本指引重點介紹了各國開發數位身分生態系統的幾種具體方式，使它們能夠減輕第 4 章所述風險，同時獲得這些系統的效益。首先，各國應遵循「永續發展的身分識別原則」，該原則現已得到 25 個以上國際組織、發展機構和其他合作夥伴的認可。[60] 雖然這些*原則*是為了支援開發政府認可的「優質」身分識別系統，但它們的應用範圍更廣，適用於公共和私人提供和使用的身分識別系統及服務。

表 3 確定永續發展原則

	原則
包含： 普遍的適用範圍和可及性	1. 確保從出生到死亡的個人獲得普遍使用權，不受歧視。 2. 消除取得和使用的障礙以及資訊和技術可用性的差距。
設計： 穩健、安全、盡責和永續	3. 建立可靠、唯一、安全和準確的身分。 4. 建立一個可互通並回應各種使用者需求的平台。 5. 使用開放標準並確保提供者和技術中立。 6. 透過系統設計來保護使用者隱私和控制權 7. 在不影響可存取性的情況下規劃財務和營運的永續性
治理：藉由保護隱私和使用者權利來建立信任	8. 透過全面的法律和法規架構保護資料隱私、安全和使用者權利。 9. 建立明確的機構職責和當責制度。 10. 透過獨立的申訴監督和裁決機制，加強法律和信任架構。

60 世界銀行。2017. *永續發展的身分識別原則：邁向數位時代*。美國華盛頓特區世界銀行集團。id4d.worldbank.org/principles。背書組織的清單可參見網站。

目標 1 確保普惠性

前兩個原則旨在支持 SDG 16.9，確保 ID 系統不遺漏任何人。*原則 1* 要求各國履行其義務，按照國際法和公約及其各自的立法架構規定，從出生到死亡並向所有人提供合法身分識別，而不僅僅是公民。這包括對在其領土或司法管轄區內出生的個人一律提供出生登記的承諾，並且擴展到數位 ID 系統，尤其上述是存取基本公共和私營部門服務（例如銀行、SIM 卡和現金轉帳）的先決條件。

有鑑於特定群體非常難以取得身分服務（尤其是數位服務），*原則 2* 要求從業人員識別並減緩在註冊、使用數位 ID 系統方面的法律、程序和社會障礙，特別關注因文化、政治或其他原因而可能遭排除的貧困人群和群體（例如婦女和性別少數群體、兒童、農村人口、少數民族、語言和宗教群體、身心障礙者、移民、被迫流離失所、和無國籍人士）。此外，數位 ID 系統和身分資料不應用作歧視或侵犯個人或集體權利的工具。

目標 2 設計出穩健、安全、靈敏且永續的 ID 系統

除了提供通用的適用範圍之外，數位 ID 系統也應具有防詐欺和防錯功能，有益於利害關係方和永續發展，同時也應保護使用者隱私並採用開放標準以促進創新，並避免發生供應商和技術鎖定現象。

具體而言，*原則 3* 指出，準確、最新的身分資訊對於確保

交易中使用的身分和屬性的可信賴性至關重要。另外，身分必須在特定環境中具有唯一性，避免重複的身分或使用可歸屬於多個人的識別符。此外，數位 ID 系統必須具有防止篡改（變更或對資料或憑證進行其他未經授權的變更）、身分盜用、資料濫用以及避免整個身分生命週期中發生其他錯誤的保護措施。

原則 4 強調了對識別和身分驗證服務的靈活性、可擴展性，並滿足人員（使用者）和信賴方（例如公共機構和私人公司）的需求和關注。為了確保與身分相關的系統和服務滿足特定的使用者需求，從業人員應在規劃和實施流程的同時與公眾和重要的利害關係方交流。數位身分識別系統對信賴方的價值大致取決於國內外的可攜權和與多個實體的互通性（取決於適當的隱私和安全保護措施）。

特別是政府認可的數位 ID，*原則 5* 進一步強調提供者保持中立的必要性，如此可提高靈活性並避免不適合特定目的或不符合政策及開發目標的系統設計。這就需要強有力的採購指導方針，以促進競爭和創新，並防止可能的技術和提供者「鎖定」，因為這會增加成本並降低靈活性，無法有效適應隨著時間的變化。此外，開放式設計原則可促進市場導向的競爭和創新，對於提高數位 ID 系統的效率和功能以及持久的互通性至關重要。同樣，開放式 API 確保數位 ID 系統環節（例如特定類型的憑證）更換時可將中斷減至最少，以支持有效的資料交換和可攜權。

除了具有回應能力和靈活性的架構外，*原則 6* 強調數位 ID 系統必須透過系統設計來保護人們的隱私並控管資料。這對於減輕本指引第 4 節所述的眾多隱私和資料保護風險至關重要。在設計時考慮民眾的隱私，意味著力求讓人們無需採取任何措施就能保護個人資料。預設情況下，應透過技術標準和預防性商業實務來保護資訊，防止其被濫用或未經授權使用。這些措施應以強而有力的法律架構輔助（如以下*原則 8* 中所強調）。

例如，蒐集和用於識別和驗證的資料應合乎使用案例的規模，並根據全球資料保護規範（如 OECD 的公平資訊慣例（FIP））和新興國際最佳規範進行管理，例如歐盟的《通用資料保護條例》（GDPR）或《加州消費者隱私法》。身分驗證協定應只就所聲稱的身分提供「是或否」的確認，若經 AML 或 CCC 相關法律的強制要求，則僅應揭露交易所需的基本資料。驗證方法應反映對交易風險等級的評估，並可採用公認的國際保證等級標準和架構。此外如非必要，憑證和識別符編號系統不應洩露敏感的個人資訊（例如參考編號應隨機產生）。

原則 7 強調必須設計出財務永續和營運永續的公部門系統，同時仍保持民眾和信賴方的存取能力。這可能涉及不同的商業模式，包括收取合理和適當的身分驗證服務費，為使用者提供增強或更快速的服務、精心設計和管理的公私合營夥伴關係（PPP）、提高效率和生產力來彌補成本、減少

洩漏，以及運用其他資金來源等，前提是不影響相關目標，亦即提供人人可用且能滿足民眾和信賴方需求的身分證明機制。

目標 3 保護隱私和使用者權利以建立信任

最後一組原則涉及如何管理數位識別系統，以保護使用者的隱私和權利、系統安全以及明確的當責和監督。

原則 8 規定了全面法律架構的要求。數位 ID 系統必須以政策、法律和法規為基礎，其應促進系統的可信度、確保資料隱私和安全性、減少濫用（例如違反正當程序且未經授權的監視），並確保提供者承擔責任。這通常包括數位 ID 系統本身相關的授權法律法規，以及相關資料保護、數位或電子政務、電子交易和商務、防制洗錢、民事登記、限定用途 ID 系統及資訊自由等各方面的法律法規。

數位 ID 系統的授權法律和法規應載明系統的宗旨、組成部分、不同利害關係方的角色和職責，如何蒐集資料、數位 ID 持有人（主體）和信賴方的責任和追索權、資料開放共用的條件、糾正不正確的資料屬性，以及如何保持包容和非歧視。有關資料保護和隱私的法律法規也應要求獨立監督機構（例如國家隱私委員會）的監督，其應具有適當的權力，以保護主體免遭第三方在未經知情同意或未依合法目存取其資料並用於商業監視或解析。架構要求在監管和自我監管模式之間保持適當的平衡，避免扼殺競爭、創新

或投資。

此外，*原則 9* 強調了在數位 ID 系統治理中需要明確的機構授權和當責制。全生態系統的信任架構都必須確立並規範 ID 系統的治理安排。其中應包括規定參與方之間機構關係的條款和條件，以便各方均清楚瞭解彼此的權利和責任。在身分識別系統提供者的角色和職責方面，應該有明確的當責制和透明性。

最後，*原則 10* 強調身分識別系統應清楚載明如何監督這些法律和法規要求。身分識別系統的使用應予以獨立監控（項目包括效率、透明度、排除、濫用等），以確保所有利害關係方適當使用身分識別系統來實現預期目的、監控和因應潛在的資料外洩，並接收個人投訴或有關個人資料處理的疑慮。此外，提供者如果不能順利解決有關識別和使用個人資料的爭議（例如拒絕登記個人身分或更正資料，或個人法律地位遭不利判決），則應由獨立且具糾正權的行政和司法主管機關迅速和低成本的審查。

附錄 D：數位 ID 保證架構和技術標準制訂機構

此列表不包括制訂國家級架構標準的 eIDAS 和 NIST 等國家或地區機構 - 參見附錄 E。

國際標準化組織（ISO）是位於日內瓦的獨立國際組織，成員為 163 國家標準實體（每國一員），該組織制訂了自願性質、基於共識、與市場相關的國際標準，據以提供產品規格、服務和系統，以確保品質、安全和效率並支持創新。一些相關標準包括：身分證明和自然人註冊（ISO/IEC 29003：2018）；實體驗證保證架構（ISO/IEC 29115：2013- 修訂中），以及運用《風險管理指引》（ISO 31000：2018）來因應身分相關風險。該組織最近召集的 TC68[61]ISO 第 7 工作組正在制訂有關自然人識別的全球標準，其中也涵蓋數位環境的應用規範。

國際電信聯盟（ITU）是聯合國資訊和通訊技術（ICT）專門機構，其成立旨在促進國際通訊網路的連結程度。ITU 分配全球無線電頻譜和衛星軌道，並制訂技術標準以確保 ICT 網路和技術在全球順暢互連。

全球資訊網聯盟（W3C）是一間國際組織，致力於為網際網路開發和推廣各種自願性質、基於共識的開放技術標準和協定，以支持互通性、可擴充性，穩定性和靈活性。在數位 ID 領域，W3C 使用生物辨識技術、行動裝置和 FIDO

---

61 ISO/TC68 是 ISO 內部的技術委員會，負責制訂和維護涵蓋銀行、證券和其他金融服務領域的國際標準。

安全金鑰為 MFA 開發了 Web 身分驗證瀏覽器 / 平台標準，並且正在開發用於分散式身分識別系統中的身分聲明驗證標準。

線上快速身分驗證（FIDO）聯盟是一間產業協會，致力推廣有效、易於使用的強式身分驗證解決方案，方法是開發技術規格來定義開放、可擴展、可互通的使用者身分驗證機制、實施產業驗證計畫，以利確保在全球順利採用相關規格；並將成熟的技術規格提交給公認的標準開發組織（例如 ISO、ITUX.1277 和 X.1278）予以正式標準化。FIDO 也透過旗下的身分驗證和綁定工作小組（IDWG）參與驗證機制。

OpenID Foundation（OIDF）是一間技術中立的非營利貿易組織，致力於推廣基於開放標準的數位 ID 服務普及化。

GSMA 是行動通訊網路營運商的全球產業協會，並且參與了適用於行動通訊平台的各種技術標準的開發，其中包括使用者身分識別和驗證的標準。

歐洲電信標準協會（ETSI）是與 CEN 和 CENELEC 並列的歐洲三大標準機構之一。ETSI 為成員提供開放、包容的環境，著眼於整體產業和社會各領域的 ICT 系統和服務需求，據以支援開發、核准和測試適用的全球標準。ETSI 向來致力於身分證明數技術，主要著重於 eIDAS 定義的信任服務，並可能將應用範圍擴及其他領域（例如 eID 和客戶審查流程的核發）。ETSI 制訂一套標準來實施 PSD2 的 RTS 規定，採用 eIDAS 定義的合格憑證來識別付款交易中的第三方（TPP）。

附錄 E：美國和歐盟數位保證架構和技術標準概述

NIST– 美國

- 身分保證等級（IAL）是指 ID 證明流程的可靠性，係依據其所需的技術數位 ID 要求來判定。依可靠性遞增順序排列，ID 證明的保證等級分別為 IAL1、IAL2、IAL3；
- 身分驗證保證等級（AAL）是指身分驗證流程的可靠性。依可靠性遞增順序排列，身分驗證（和憑證生命週期管理）的保證等級分別為為 AAL1、AAL2、AAL3；
- 聯合識別保證等級（FAL）（如果適用）是指聯合網路的可靠性，所謂的聯合網路則是在聯合環境中傳達身分驗證結果和 ID 屬性資訊的聲明的可靠性（強度）。依可靠性遞增順序排列，聯合識別的保證等級分別為 FAL1、FAL2、FAL3；

身分證明

說明欄 18 利用 NIST 數位 ID 技術標準來評估 ID 證明的可靠性

IAL1- 不需要將申請人連結到特定的真實身分 - 即不需

要 ID 證明，因此無法保證申請人確實具有其所聲稱的身分。這表示：

- 不需要身分屬性；
- 申請人可以但不需要自行聲明身分屬性。
- 任何提供或蒐集的身分屬性皆為（或視為）自我斷言，並不予以確認或驗證。

IAL2- 身分證明真實性的可信度較高；其包含準確的屬性資訊；且與申請人具有關聯性。

- 身分屬性證據是依據證據品質（弱效、普效、強效和優效）及所憑藉的文件或數位資訊數量予以蒐集。
- 身分證明經確認真實無誤。
- 身分證據及其身分屬性可證實所聲明的身分實際存在，並且
- 身分證明經過驗證，可確認待查身分與個人（申請人）相關聯，包括確認地址正確無誤
- 允許進行遠端或面對面的身分證明。注意：在 NIST 數位 ID 標準中，「親自進行」的身分證明方式包括**在監督下與申請人進行遠端互動**，以及申請人和身分服務提供者實際位於同一位置的互動（請參見下文討論）。
- 生物辨識屬於非強迫性質

- 如果個人無法滿足常規身分證明要求（例如無法出具合格的身分證據），可以使用可信公證人協助申請人進行身分證明。
- 身分屬性的證據必須滿足規定的證據品質要求，允許在特定強度下依規定特徵決定所需數量證據的各種組合。

IAL3- 身分證據真實準確，可信度極高；身分屬性確實為個人所擁有，且申請者即是該名個人，且可適當關聯至現實世界中的身分。

- 身分證明程序必須親自進行；請注意：「親自進行」的身分證明方式包括在監督下與申請人進行遠端互動，以及申請人和身分服務提供者實際位於同一位置的互動。（請參閱第 III 節「非面對面的客戶引導」）
- 身分證據的品質要求更嚴格
  - o 需要更多強度較高的身分證明文件
  - o 生物辨識是強制規定。需要生物辨識身分屬性和生物辨識流程來偵測詐欺性或重複註冊，並將其視為待驗身分綁定到憑證機制
- 身分屬性必須由經過授權和培訓的憑證服務提供者（CSP）代表進行驗證。

資料來源：美國 NIST 標準

表 4IAL1、IAL2 和 IAL3 身分證明規定摘要

要求	IAL1	IAL2	IAL3
存在	無要求	面對面且不受監督的遠端模式。	面對面且受監督的遠端模式。
解析	無要求	• 完成身分解析所需的基本屬性。 • 可使用 KBV 增加可信度。	與 IAL2 相同
證據	未蒐集身分證明。	• 1 項優效或強效證據（取決於原始證據強度和核發來源確認結果） • 2 項強效證據，或 • 2 項強效證據加上 2 項普通效力證據。	• 2 項優效證據，或 • 1 項優效證據和 1 項強效證據（取決於原始證據強度和核發來源確認結果） • 2 項強效證據加 1 普效證據。
確認	無確認	必須使用與所提供證據相同強度的流程來驗證每個證據。	與 IAL2 相同
確認	無驗證	經過能夠達到強效等級的流程驗證。	經過能夠達到優效等級的流程驗證。
地址確認	無需地址確認	必需項目。發送到任何記錄地址的註冊碼。以不同於註冊碼的方式發送的通知。	必需項目。郵寄地址證明的通知。
生物特徵蒐集	否	選擇性	強制性
安全控制項	不適用	• 中等基準（或等效的聯合識別或產業標準）。	• 高等基準（或等效的聯合識別或產業標準）。

說明欄 19 面對面的身分證明和註冊

如上所述，該技術標準允許在 IAL2 等級親自進行身分證明，在 IAL3 則是強制規定親自進行。重點在於（包括有利於普惠金融目標的關鍵），親自進行的身分證明和註冊可以透過以下方式進行：

- 在操作人員的監督下與申請人當場互動；或者
- 在操作人員的監督下與申請人*遠端互動*，其所依循的遠端親自進行身分證明機制可達到與現場（實體互動）身分證明相當的可信度和安全性。

對於這兩種親自進行的身分證明機制，技術標準均要求（1）操作人員必須在證明流程中檢查生物特徵來源（例如手指、臉部）是否存在人工物質；（2）CSP 必須確保從申請者本人而非其他主體蒐集生物特徵，並遵守標準規定的所有生物辨識效能要求。

在監督下遠端進行身分證明和註冊的可比性要求

為了在「監督下親自遠端進行」以及「申請人與 CSP 位於相同實體位置」這兩種身分證明和註冊方式之間建立可比性，必須達到以下要求（除了 IAL3 確認和驗證要求之外，如上所述）：

CSP 必須：

- o 完整監控身分證明過程（例如申請人的連續高解析度視訊傳輸）。
- o 讓現場操作員與申請人遠端參與完整的身分證明過程。操作員必須經過培訓，才能發現潛在的詐欺行為並正確在虛擬環境下執行證明流程。
- o 由整合的掃描儀和感測器對所有證據進行數位驗證（例如透過晶片或無線技術）。
- o 確保所有通訊都在相互驗證的受保護管道上進行。
- o 配合身分證明流程進行的環境，採用適當的實體防篡改和抗破壞功能（例如在限定區域內的自助服務機或由受信任人士加以監督，這類措施所需的實體篡改偵測機制會少於半公共區域，例如購物商場大廳）。

申請人必須連續保持（不能離開）受監督的身分證明流程，而且在遠端證明的過程中，申請人所有操作均必須清晰可見。

說明欄 20 身分驗證和生命週期管理

驗證保證等級（AAL）設定下列兩方面的技術要求：（1）驗證協定和流程（包括憑證和驗證者的發布和綁定）和（2）驗證機制的生命週期管理（包括在遺失或遭竊、有效期屆滿 / 失效及重新綁定時註銷）。面對強式身分驗證機制（更高的 AAL），不肖份子需要更強的能力並花費更多資源才能破壞身分驗證流程。較高 AAL 等級的身分驗證可以有效降低冒名頂替、重播和其他攻擊的風險，以免主體的數位 ID 遭到詐欺性冒用。AAL 包括驗證者類型的技術要求；核准的加密技術和安全的身分驗證管道（包括入侵偵測、模擬和重播抵禦要求）、重新驗證（擴大範圍）訂戶驗證流程、記錄保留、網路安全和隱私。AAL 也確立以下要求：將身分驗證機制綁定到經證實的身分，並且在訂戶身分驗證機制綁定後採取行動，來因應的整個生命週期中可能發生的事件，包括遺失、遭竊、未授權複製、過期和註銷，進而建立驗證機制的可信度。這些要求中許多都需使用大量技術，並且合併參照其他高度客戶資料保密標準。

下列摘要概述各種 AAL 身分驗證的若干要求。詳細討

論請參見 NIST 800-63（b）。

- AAL1：提供*某種保證*，即申請者（聲明 [主張] 身分以要求帳戶授權的個人）控制訂戶帳戶所綁定的身分驗證機制。AAL1 允許在*較低的*基準範圍內使用多種身分驗證技術、身分驗證機制類型和客戶資料保密控制。MFA 屬於非強迫性質）。單憑生物辨識技術即可用作 AAL1 的單因素身分驗證機制。
- AAL2：申請者控制與客戶 / 訂戶帳戶所綁定的身分驗證機制，進而提供*高可信度*。其需要 MFA（多因素身分驗證機制或 2 項單因素身分驗證機制），其遵循的身分驗證協定整合了採用經核准的特定加密技術與*中等*基準的客戶資料保密控制項。AAL2 對身分驗證機制類型的要求比 AAL1 更為嚴格。[62] 生物辨識可以用作一項身分驗證*因素*（您所擁有的東西），而裝置可以作為第二項身分驗證因素（您所擁有的事物），但不能用作唯一的身分驗證者類型。
- AAL3：申請者控制訂戶帳戶所綁定的身分驗證機制，*具有很高的可信度*。AAL3 要求 MFA 既使用硬體驗

[62] AAL2 允許使用以下任何一種多因素身分驗證機制：多因素 OTP 裝置、多因素加密軟體或多因素加密裝置。當使用 2 項單因素身分驗證機制的組合時，其中一項身分驗證機制必須是記憶的秘密，另一項必須是所有物（即「您擁有的事物」）並使用以下任何一種方法：查找秘密、頻外裝置、單因素 OTP 裝置、單因素加密軟體；或單因素密碼裝置。

證機制，同時採用另一種驗證機制，其一據經核准的密碼協定證明持有金鑰，藉此提供驗證方偽裝抗性（VIR）。[63] 申請者必須使用認可的加密技術透過安全的身分驗證協定，來證明擁有和控制兩項不同的身分驗證因素。驗證機制必須具備驗證方偽裝抗性，對重播的防禦力以及對相關旁路攻擊的抵抗力。使用生物辨識因素時，身分服務提供者（驗證方）必須自行確定生物辨識感測器和後續處理是否滿足指定的效能要求。CSP 必須以*較高的*基準採用適當定製的安全控制措施。

eIDAS– 歐洲聯盟

eIDAS 架構針對已公告電子身分識別方案架構下的電子身分識別方法提供了三項保證等級：低度、實質和高度。2015 年 9 月 8 日的歐盟執委會實施條例（EU）2015/1502 為每個等級設置了最低安全規範。本實施法案規定的規範和程序考量了國際標準 ISO/IEC 29115，因其是電子身分識別保證等級範圍內可用的主要國際標準；而 eIDAS 條例內

63 申請者使用身分驗證機制所儲存的私鑰來證明自己擁有並控制身分驗證機制。IDSP（驗證者）透過某種憑證（通常是公開密鑰憑證）得知申請者的公開密鑰，其使用核准的加密驗證協定來驗證申請者是否擁有和控制相關私鑰驗證機制，並向 RP 判斷該人已證實身分。

容有別於國際標準，尤其在身分證明和驗證要求方面，以及成員國身分安排方式與歐盟現有相同用途工具之間的差異。在歐盟 / 歐洲經濟區國家，如果公共部門機構要求存取其線上服務中一項實質或高度保證的電子身分，則必須接受保證等級相同或更高的所有電子身分驗證方法，且必須關聯至歐盟執委會已公告的身分驗證機制（發布在歐盟官方公報上），方可取用此線上服務。此外，公部門機構可以自願決定承認較低保證等級的電子身分識別方案。

出於 eIDAS 的目的，數位 ID 系統的環節為：

- **註冊**旨在確保唯一代表自然人或法人的身分，或是由自然人代表法人的身分。註冊涉及不同步驟：
  - o 申請和登記：（1）確保申請人瞭解電子身分識別工具使用條款和條件。（2）確保申請人瞭解有關電子身分識別的建議安全預防措施。（3）蒐集身分證明並驗證所需的相關身分資料。
  - o 身分證明和驗證機制包括 ID 文件的真實性和有效性驗證，其可關聯至真實個人，以及驗證該人身分即是其所聲稱身分。
- **電子身分識別**方法旨在管理、處理驗證因素的數量和性質、是否設計為僅當所屬人員控制或擁有、註銷和更新的情況下方可使用。
- **身分驗證**列出了有關身分驗證機制的每項保證等

級的要求，自然人或法人據以使用電子身分識別工具向信賴方確認其身分。

- **管理和組織**，所有跨境提供電子身分識別相關服務的參與者，都應有成文的客戶資料保密管理慣例、政策、風險管理方法和其他公認控制措施，據此向各國電子身分驗證計畫的適當治理機構保證採行有效的實務。

四個階段依下列標準定義了三項保證等級：低度，實質和高度：

- **低度** – 所聲稱或主張的個人身分可信度有限，其特徵是參考與其相關的技術規格、標準和程序（包括技術控制），旨在降低身分濫用或變更的風險；
- **實質** – 聲稱或主張的個人身分具有實質可信度，其特徵是參考與其相關的技術規格、標準和程序（包括技術控制），旨在降低身分濫用或變更的風險；
- **高度** – 聲稱或主張的個人身分可信度高於實質保證等級的電子身分識別方法，其特徵是參考與其相關的技術規格、標準和程序（包括技術控制），旨在避免身分濫用或變更的風險。

依據一般預設，如果依據已公告的電子身分識別機制核發的電子身分識別方法符合較高保證等級的要求，則自動符合較低保證等級的等效要求。

表 5eIDAS 保證等級下的驗證要求

保證等級	所需條件
低	• 在發佈人員識別資料之前，需要對電子身分識別裝置及其有效性進行可靠的驗證。 • 如果身分驗證機制會儲存個人身分識別資料，則該資訊可受到保護，以免遺失和損害（包括離線分析）。 • 身分驗證機制支援驗證電子身分識別方法的安全控制功能，因此具備基本強化（enhanced-basic）攻擊能力的攻擊者不太可能藉由猜測、竊聽、重播或操縱通訊之類的活動來破壞驗證機制。
實質	低度等級，再加上： • 在釋出個人識別資料之前，需要透過動態身分驗證機制對電子身分識別裝置及其有效性進行可靠的驗證。 • 身分驗證機制支援驗證電子身分識別方法的安全控制功能，因此**具備中等（moderate）攻擊能力**的攻擊者不太可能藉由猜測、竊聽、重播或操縱通訊之類的活動來破壞驗證機制。
高度	實質等級，再加上：身分驗證機制支援驗證電子身分識別方法的安全控制功能，因此**具備高度（high）攻擊能力**的攻擊者不太可能藉由猜測、竊聽、重播或操縱通訊之類的活動來破壞驗證機制。

詞彙表

應用程式：旨在幫助使用者執行特定任務的電腦軟體。

應用程式介面（API）：用於構建和整合應用程式軟體的一組定義和協定。API 使數位產品或服務可以輕鬆地與其他產品和服務進行通訊。

保證等級：是指數位 ID 流程三個階段各別的可靠性或可信度等級。請參閱本報告第 2 節的技術標準概述以及第 5 節「利用數位 ID 技術標準實施風險基礎方法」。

屬性證據可以是實體（文件）或純數位性質，或者是數位格式的實體屬性證據（例如紙本或塑膠駕駛執照的電子掃描檔）。

身分驗證旨在確立主張身分的申請者就是在引導期間取得、驗證並憑證化身分證明的同一人。

身分驗證機制是申請者擁有和控制的事物，用於驗證（確認）申請者是核發憑證的對象，亦即（取決於數位 ID 系統的驗證環節強度）是實際訂戶和帳戶持有人（依身分驗證保證等級指定不同程度的可能性）。

生物辨識

- 生物物理學特徵屬性，例如指紋、虹膜紋理、聲紋和臉部識別，此皆為靜態屬性。

- 生物力學生物辨識：這類屬性（例如擊鍵力學）是個人肌肉、骨骼系統和神經系統獨特交互作用的產物，皆為動態屬性。
- 行為生物辨識屬性：是依據社會物理學門下的新分支「運算社會科學」（computational social science）得出的研究成果，包括個人各種行動和使用方式的地理空間時態資料流，例如個人電子郵件或簡訊格式、檔案存取日誌、行動電話使用、地理位置模式。

蒐集和解決是身分證明的一部分，涉及取得屬性、蒐集屬性證據（識別符）；並將身分證據和屬性解析為特定族群或脈絡中的個別唯一身分。

連續驗證是動態形式的身分驗證。其可利用生物力學生物辨識、行為生物辨識模式及 / 或動態交易風險分析，專注於確保在與個人線上互動期間蒐集的特定資料點（例如地理位置、MAC 和 IP 位址、鍵入節奏和行動裝置角度）在整個過程中皆符合預期。

申索人是指試圖證明自己的身分以取得該身分相關權利（例如開設或存取金融帳戶）的個人。申索人也可以稱為訂戶，後者申明自己對於信賴方（RP）身分的擁有權，並尋求使用身分驗證協定對此進行驗證。

憑證是一種實體物件或數位結構，透過一或多個識別符將訂戶經證實的身分授權綁定到訂戶擁有和控制的至少一個身分驗證機制上。

憑證服務提供者（CSP）：這類實體負責向訂戶核發及 / 或註冊身分驗證機制和相應電子憑證（將身分驗證機制綁定到已驗證身分）。CSP 負責在憑證的整個生命週期中維護訂戶的身分憑證和所有相關的註冊資料，並負責向驗證者提供有關憑證狀態的資訊。

憑證填充（也稱為違規重播或列表清除）：網路攻擊的類型，將遭竊帳戶憑證（通常是由於資料外洩）在其他系統上進行匹配測試。如果受害者為另一個帳戶設定相同密碼（在資料外洩中遭竊），則該帳戶可能遭入侵得逞。

重複資料刪除：將身分證據和屬性解析為特定族群或脈絡中個別唯一身分的流程。

依本指引定義，**數位 ID 系統**是涵蓋身分證明 / 註冊和驗證流程的系統。身分證明和註冊可以是數位或實體性質（文件），也可以是兩者的組合，但是綁定、憑證、身分驗證和可攜權 / 聯合識別必須是數位性質。

數位 ID 保證架構和技術標準是一套開源、共識導向的數位 ID 系統保證架構和技術標準，而此架構標準是由多個司法管轄區、國際組織和產業機構所擬定，詳見***附錄 D：數位***

ID 保證架構和技術標準制訂機構。NIST 標準和 eIDAS 法規範例請參閱附錄 E：美國和歐盟數位保證架構和技術標準概述。

eIDAS 規章：歐盟第 910/2014 號「電子交易在內部市場的電子身分識別驗證和信託服務規則」。

註冊是指 IDSP 將已證實身分的申請人登記（註冊）為「訂戶」並建立其身分帳戶的流程。該流程使用適當的綁定協定，將訂戶的唯一已驗證身分（即訂戶屬性 / 識別符）授權**綁定**到訂戶擁有和控制的一或多個身分驗證機制。將訂戶身分綁定到身分驗證機制的流程也稱為「**憑證化**」。

聯合識別是指使用聯合數位架構和判斷提示協定在一組網路系統之間傳遞身分和身分驗證資訊。

通用身分識別系統（或基礎身分識別系統）通常提供文件及 / 或數位憑證，受到政府機構和私營部門服務提供者廣泛認可並接受，用作各種目的正式身分證明（例如國家 ID 系統和民事登記資料庫）。

身分證據 – 請參閱屬性證據。

身分生命週期管理是指因應身分生命週期中可能發生的事件而應採取的行動，這些事件會影響身分驗證機制的使用、安全性和可信度，例如驗證機制及 / 或憑證的遺失、遭竊、未經授權的複製、到期和註銷。

身分證明釐清的問題是：「您是誰？」，在這項流程中，身分服務提供者（IDSP）蒐集、驗證和確認某人的相關資訊，並將其解析為特定族群或脈絡中的唯一個體。它涉及三項動作：（1）蒐集 / 解析、（2）確認和（3）驗證。

身分服務提供者（IDSP）：這是一項通用總稱，泛指提供和操作數位 ID 系統或解決方案流程和環節的各種實體。IDSP 為使用者和信賴方提供數位 ID 解決方案。個別實體可以承擔一或多項 IDSP 的功能角色 - 請參閱***附錄 A：基本數位身分系統及其參與者之說明***，以概括所有相關實體，包括 – 身分提供者、憑證服務提供者（CSP）、註冊機構（RA）（或身分管理者）、驗證方、使用者 / 個人、申索人、訂戶、申請人、信賴方和信任架構提供者 / 信任機構。

冒名頂替是假冒真實個人身分的行為，可能是單純使用外貌相似者的遭竊文件，但也可能是結合偽造證明文件的虛假身分（例如使用冒名頂替者的肖像替換護照上的照片）。

限定用途 ID 系統（也稱為功能型 ID 系統）旨在為特定服務或部門（例如稅務管理）提供識別、驗證和授權功能；取得特定政府福利和服務；表決；授權操作機動車輛；（在特定司法管轄區）取得金融服務等。功能型 ID 系統的範例包括（但不限於）：稅籍號碼、駕駛執照、護照、選民登記卡、社會保險碼和難民身分證明文件。

中間人攻擊：試圖達到網路釣魚相同的目標，並且可以作為網路釣魚工具，但方式是攔截受害者與服務提供者之間的通訊。

多因素身分驗證（MFA）結合使用 2 項以上身分驗證因素來增強安全性。

NIST 標準 / 指引：美國國家技術標準局 800-63 數位 ID 指引。

在本指引中，**正式身分**是唯一自然人的限定概念，該自然人（1）其基礎為某些個人特徵（屬性或識別符），可在群體或特定環境脈絡中確立該人的獨特性，以及（2）由國家基於監管和其他正式用途所認可。

個人身分資訊（PII）包含任何可以單獨或與其他資訊結合使用以識別特定個人身分的資訊。

網路釣魚（也稱為中間人攔截或憑證攔截）是一種詐欺性嘗試，使用詐騙電子郵件和網站蒐集不知情的受害者的憑證。例如，犯罪分子試圖誘騙受害者向貌似可信來源提供姓名、密碼、政府身分證號碼或憑證。

PIN 碼擷取和重播是使用鍵盤記錄器擷取電腦鍵盤上輸入的 PIN 碼，並在使用者未察覺的情況下，趁智慧卡插入讀卡機時，使用擷取的 PIN 碼來存取服務）。

可攜權 / 互通性：可攜式身分是指個人的數位 ID 憑證可在無關聯的公私部門實體業務往來中用於證明正式身分，而

無需每次都要取得和驗證個人身分資訊（PII）並進行客戶識別 / 驗證。可攜權要求開發可互通的數位識別產品、系統和流程。可攜權 / 互通性可由不同的數位 ID 架構和協定予以支援。

漸進式身分：隨著個人身分的數位足跡日益穩健，其正式身分會逐漸變化，且數位足跡會提供越來越多的屬性及 / 或身分驗證機制，可以針對越來越多的來源和範圍進行驗證。

正式身分認證通常取決於政府提供或核發的某種註冊、文件或認證（例如出生證明、身分證或數位 ID 憑證），其構成了核心識別符或屬性（例如姓名、性別、出生日期和地點）的證據，用於確立和驗證正式身分。證明「正式身分」的標準可能因司法管轄區而異。

公共金鑰加密（用於公鑰基礎結構（PKI）憑證）：可為一個實體（個人、系統或裝置）產生一對金鑰，由該實體安全地持有私鑰，同時將公鑰自由分配給其他實體。然後，持有公鑰的任何人都可以用它加密訊息，並放心發送給私鑰持有者，因為只有後者才能開啟此訊息。

受監管實體：在本指引中，「受監管實體」泛指金融機構、虛擬資產服務提供業（VASP）的指定之非金融事業或人員（DNFBPs），而 DNFBPs 必須在 R.22 指定的情況下進行客戶盡職審查。2019 年 6 月，FATF 修訂第 15 項建議（新

技術）和 INR15，目的包括要求 VASP 必須履行第 10 項建議所規定的客戶審查義務。

信賴方（RP）：藉由訂戶的憑證或身分驗證機制或驗證方對申請者身分的判斷提示，透過身分驗證協定來識別訂戶身分的人（自然或法人）。典型的 RP 包括金融機構和政府部門。

訂戶：這類人員的身分已由憑證服務提供者（CSP）驗證並綁定到身分驗證機制（憑證），並且可以使用該身分驗證機制來證明身分。訂戶從 CSP 接收一或多項身分驗證機制和相應的憑證，並且可以使用一或多項身分驗證機制來證明身分。

合成身分是指犯罪分子結合真實（通常藉由竊取而得）和虛假資訊假造新的（合成）身分，可以用於開設詐欺帳戶以及從事詐欺購買行為。有別於冒名頂替，這類犯罪分子偽裝的是實際上不存在的個人，而不是冒充真實存在的身分。

分層客戶盡職審查（有時稱為分層帳戶或累進**客戶盡職審查**）：根據受監管實體進行識別 / 驗證的程度，可以存取一系列不同的帳戶功能。基本的第 1 級系列服務只需最低限度的識別即可存取。僅當客戶提供所需的附加識別 / 驗證資訊時，才允許存取後續帳戶等級和其他服務（例如更高的交易限額或帳戶餘額、多樣化的存取和交付管道）。同時，

這些帳戶的服務設有限制（例如每日 / 每月提款的上限、依照客戶審查等級和客戶風險狀況決定的存款限額）。請見 FATF（2013-2017）《防制洗錢和資恐措施以及普惠金融 - 附客戶盡職審查增補條文。

可信公證人（也稱為「介紹人」）可以是經提名的個人或組織（例如公證人、法定監護人、醫療專業人員、保管人、授權書人或某種其他形式的經過培訓和核准或認證的個人）。根據司法管轄區的適用法律，法規或代理政策，為申請人提供身分證據的一種形式。這是美國 NIST 標準中使用的術語：請參閱 NIST 800-63A 4.4.2。IAL2 可信公證人證明要求。

確認是身分證明的一部份，指確定證據的真實性（不是假冒、偽造或盜用），並且對照可接受（經授權 / 可靠）的來源，檢查身分資訊 / 證據以確定資訊相符且可靠，進而判定證據包含的資訊是準確、獨立的來源資料 / 記錄。

驗證是身分證明的一部分，流程包括確認已驗證的身分可關聯到接受身分驗證的個人（申請人）。

驗證方：這類實體會使用身分驗證協定確認申索人對一或多項身分驗證機制的擁有和控制權，藉此驗證信賴方（RP）的申索人身分。

www.fatf-gafi.org

2020 年 3 月