個資管理及去識別化標準介紹

蔡敦仁
國家標準審查委員
國家標準起草委員
(TC21/SC08資訊安全分組召集人)
tsaidwen@gmail.com
中國文化大學資工系

驗證vs認證

驗證與認證有何不同？

- **認證(Accreditation)**：指認證機構(AB)給予書面正式認可(或確證與查證)驗證機構(CB)有能力執行規定工作之過程或活動
- **驗証(Certification)**：指驗證機構(CB)授予書面保證人員、產品、程序或服務符合規定要求之過程或活動
- **認證機構(Accreditation Body, AB)**：各國政府為管理驗證機構(CB)的專業與品質，成立機構加以管理，此程序稱之為認證（Accreditation）。
  - 各國幾乎均已成立獨立認證機構，例如：TAF(台灣)、UKAS(英國)、ANAB(美國)、COFRAC(法國)、CNAB(中國)、JAB(日本)、DAR(德國)及KAB(韓國)等
- **驗證機構(Certification Body, CB)**：公正獨立的第三方單位，驗證各公司或政府單位之人員、產品、程序或服務符合標準(或規定)所要求之過程或活動
  - 從事各項標準驗證的機構很多，包括SGS、BSI、ETC、TUV等

管理系統標準格式

管理系統標準(MSS)

- 品質管理系統(CNS 12681, ISO 9001)
- 環境管理系統(CNS 14001)
- 資產管理系統(ISO 55001)
- 資訊安全管理系統(CNS 27001)
- 隱私管理系統(privacy management system, PMS)或稱為個人資訊管理系統(personal information management system, PIMS)
  - BS 10012

Annex SL

- 2012由ISO發展之撰寫管理系統標準(management system standard, MSS)的指導綱要
- 提供新ISO MSS或修訂既有MSS(例：ISO 9001、ISO 27001)之框架
  - 所有新ISO MSS將遵循此框架撰寫，舊MSS將依新框架修改
- Risk-based

- MSS之結構

1. 適用範圍(Scope)
2. 引用標準(Normative references)
3. 用語及定義(Terms and definitions)
4. 組織之全景(Context of the organisation)
5. 領導(Leadership)
6. 規劃(Planning)

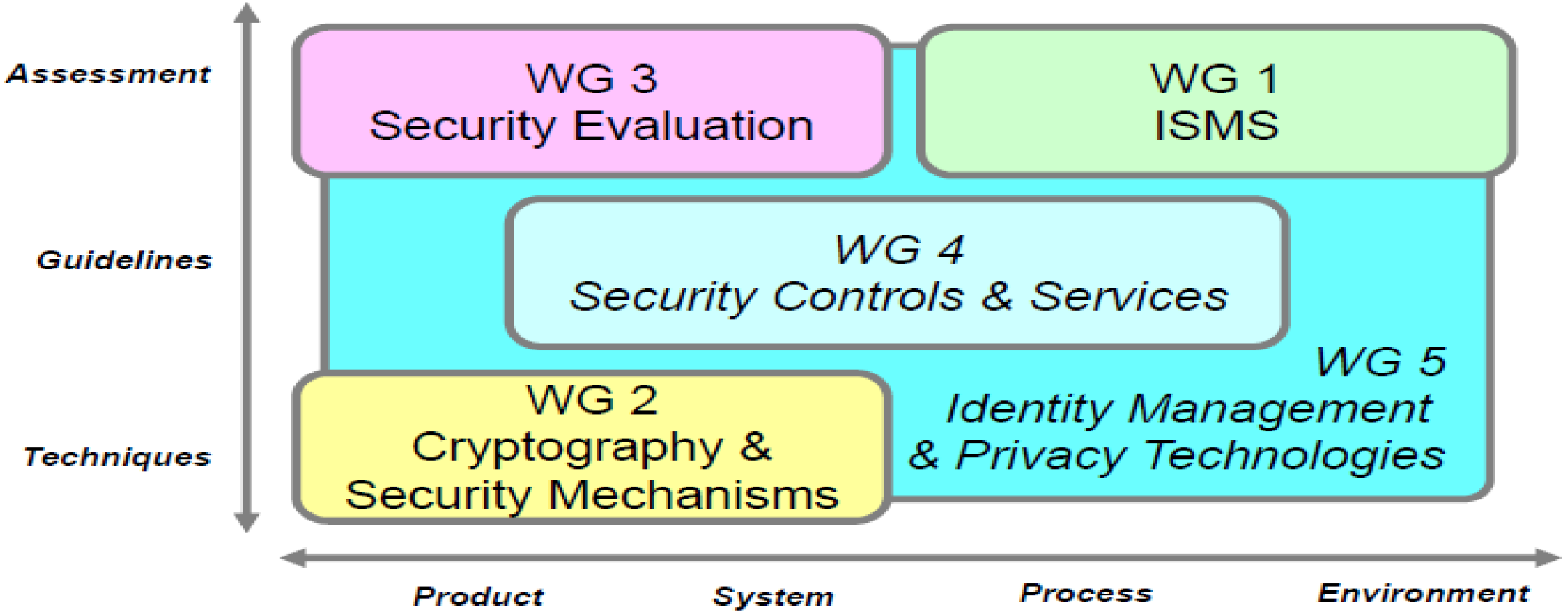
   6.1因應風險及機會之行動(Actions to address risks and opportunities)
7. 支援(Support)
8. 運作(Operation)
9. 效能評估(Performance evaluation)
10. 改進(Improvement)

ISO隱私管理相關標準

ISO標準文件狀態

- PWI – Preliminary Work Item
- NP or NWIP – New Proposal / New Work Item Proposal (e.g., ISO/IEC NP 23007)
- AWI – Approved new Work Item (e.g., ISO/IEC AWI 15444-14)
- WD – Working Draft (e.g., ISO/IEC WD 27032)
- CD – Committee Draft (e.g., ISO/IEC CD 23000-5)
- FCD – Final Committee Draft (e.g., ISO/IEC FCD 23000-12)
- DIS – Draft International Standard (e.g., ISO/IEC DIS 14297)
- FDIS – Final Draft International Standard (e.g., ISO/IEC FDIS 27003)
- PRF – Proof of a new International Standard (e.g., ISO/IEC PRF 18018)
- IS – International Standard (e.g., ISO/IEC 13818-1:2007)

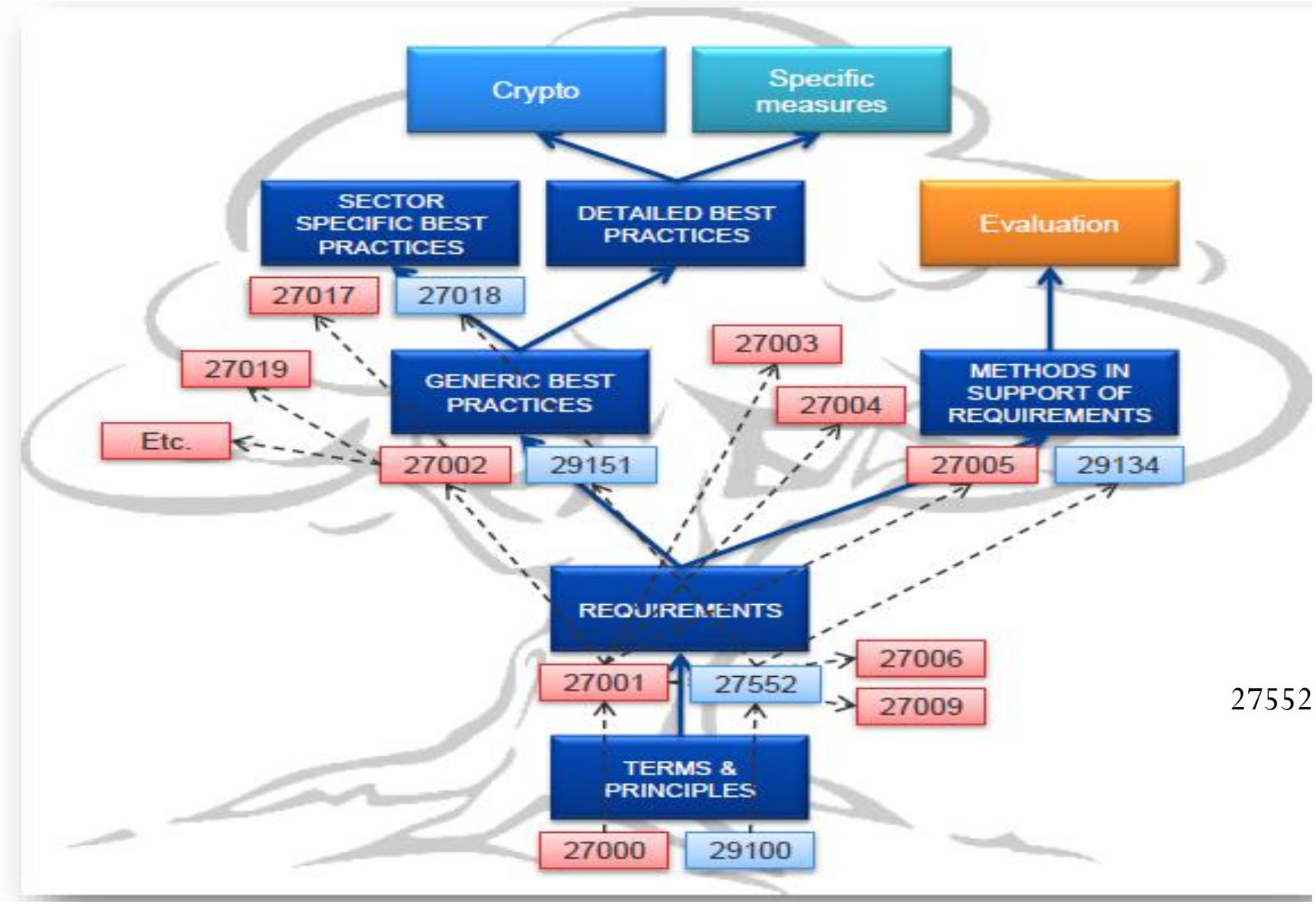
ISO/IEC JTC 1/SC 27 (IT 安全技術)各工作小組執掌



ISMS及PM之主要CNS/ISO標準

- ISMS
  - CNS 27001資訊技術-安全技術-資訊安全管理系統-要求事項
  - CNS 27002資訊技術 - 安全技術 - 資訊安全控制措施之作業規範
  - CNS 27005資訊技術 - 安全技術 - 資訊安全風險管理
  - CNS 27009 CNS 27001之產業特定應用 - 要求事項
  - CNS 27017 雲端服務資安控制措施之作業規範
  - …
- PM
  - CNS 29100資訊技術 - 安全技術 - 隱私框架
  - CNS 29191部分匿名及部分去連結鑑別之要求事項
  - CNS 29101隱私架構框架
  - CNS 29134: 隱私衝擊評鑑
  - CNS 29151: PII保護作業規範 (已有驗證)
  - CNS 27018公用雲PII 處理者保護個人可識別資訊(PII)之作業規範
  - ISO 27701
  - ISO 20889
  - …

ISO 資安與隱私主要標準架構



27552➔27701

PIMS標準制定之不同觀點

(1)獨立標準

- 例如：BS10012

(2)ISO 認為個資管理系統(PIMS)為 27001之延伸驗證

- 依據ISO 27009(ISO 27001產業特定應用：要求事項) ，納入隱私要求(ISO 29100)➔ISO 29151
- 依據ISO 27001+27002+29100+GDPR要求➔ISO 27701

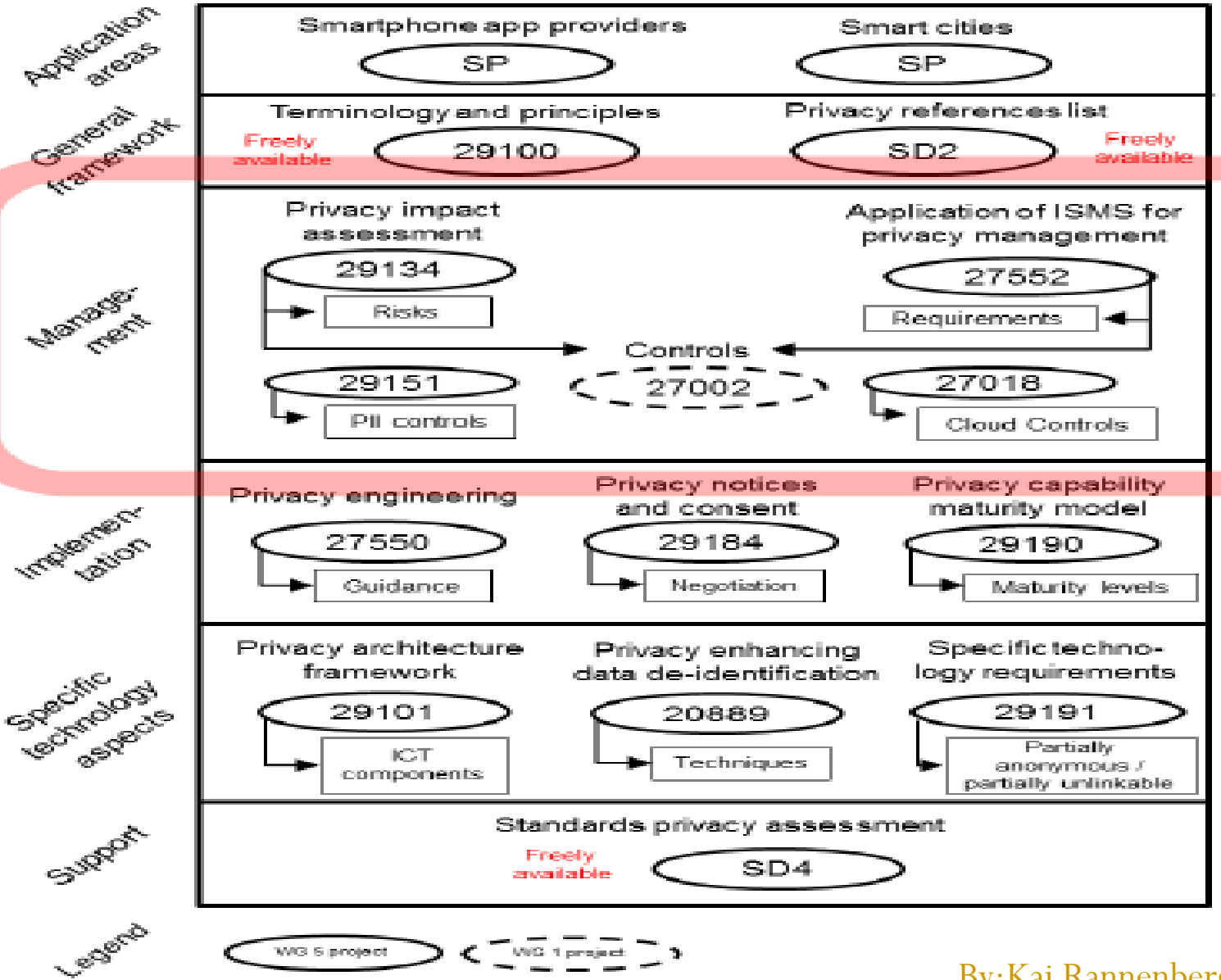
- 但各國及各地區(例：歐盟)常有法律規範個資保護，符合國際標準是否符合相關法律要求？

ISO之PMS/PIMS標準制定概念

- ISO不打算建立獨立之PMS/PIMS標準
  - 而是基於27001，增加控制措施
    - ISO 29151 Information technology -- Security techniques -- Code of practice for personally identifiable information protection
    - ISO 27701 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
    - (formerly known as ISO/IEC 27552 during the drafting period)

ISO/TEC 27009

WG 5 Privacy/PII標準 Roadmap



27552➔27701

By:Kai Rannenberg

WG 5制定標準(1/2)

- **框架及架構**
  - A framework for identity management (ISO/IEC 24760 (Parts 1-3), 2011, 2015, 2016)
  - Privacy framework (ISO/IEC 29100, IS:2011) (CNS 29100隱私框架)
  - Privacy architecture framework (ISO/IEC 29101:2013) (CNS 29101隱私架構框架)
  - Entity authentication assurance framework (ISO/IEC 29115:2013)
  - A framework for access management (ISO/IEC 29146:2016)
  - Telebiometric authentication framework (ISO/IEC 17922:2017)
- **保護概念**
  - Biometric information protection (ISO/IEC 24745, IS:2011)
  - Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, 2012) (CNS資訊技術 - 安全技術 - 部分匿名及部分去連結鑑別之要求事項)

WG 5制定標準(2/2)

- 全景及評鑑之指引
  - Authentication context for biometrics (ISO/IEC 24761:2009/Cor 1:2013)
  - Privacy capability assessment model (ISO/IEC 29190:2015)
  - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018:2014) (CNS 27018資訊技術-安全技術-公用雲PII處理者保護個人識別資訊(PII)之作業規範)
  - Identity proofing (ISO/IEC 29003:2018)
  - Privacy impact assessment – methodology (ISO/IEC 29134:2018)
  - Code of practice for PII protection (ISO/IEC 29151:2018)(CNS 29151個人可識別資訊保護之作業規範)

CNS 29100

- 資訊技術 - 安全技術 - 隱私框架
- 個人可識別資訊(personally identifiable information, PII)：所有資訊其
  (a)能用以識別此類資訊所涉及之PII當事人，或
  (b)係或得以直接或間接連結至PII當事人
- 提供下列隱私權框架
  - 規定共同隱私權術語
  - 定義處理個人可識別資訊(PII)之行為者、角色及互動
  - 隱 私 政 策
  - 隱私保 全 要 求 事 項
  - 隱私控制措施
  - 資訊技術之隱私原則

行為者及角色

- **PII當事人(PII principal)**
  - 個人可識別資訊(PII)所關聯之自然人
- **PII控制者(PII controller)**
  - 判定個人可識別資訊(PII)處理之目的及方法的隱私權相關者，而非就個人目的使用資料的自然人

  備考：PII控制者有時委派他人(例：PII處理者)，代表其處理PII，而處理之責任仍由PII控制者承擔
- **PII處理者(PII processor)**
  - 代表PII控制者並依其指示，處理個人可識別資訊(PII)之隱私權相關者
- **第三方(third party)**
  - 除PII當事人、PII控制者及PII處理者，以及經PII控制者或PII處理者直接授權處理資料之自然人外的隱私權相關者

PII 當事人、PII 控制者、PII 處理者及第三方間之PII 流向及其角色

	PII當事人	PII控制者	PII處理者	第三方
情境(a)	PII提供者	PII接收者	—	—
情境(b)	—	PII提供者	PII接收者	—
情境(c)	PII提供者	—	PII接收者	—
情境(d)	PII接收者	PII提供者	—	—
情境(e)	PII接收者	—	PII提供者	—
情境(f)	—	PII接收者	PII提供者	—
情境(g)	—	PII提供者	—	PII接收者
情境(h)	—	—	PII提供者	PII接收者

CNS 29100 之隱私原則

1.同意及選擇
2.目的適法性及規定
3.蒐集限制
4.資料極小化
5.利用、持有及揭露限制
6.準確性及品質
7.公開、透明及告知
8.個人參與及存取
9.可歸責性
10.資訊安全
11.隱私遵循

CNS 29100 vs CNS 27000

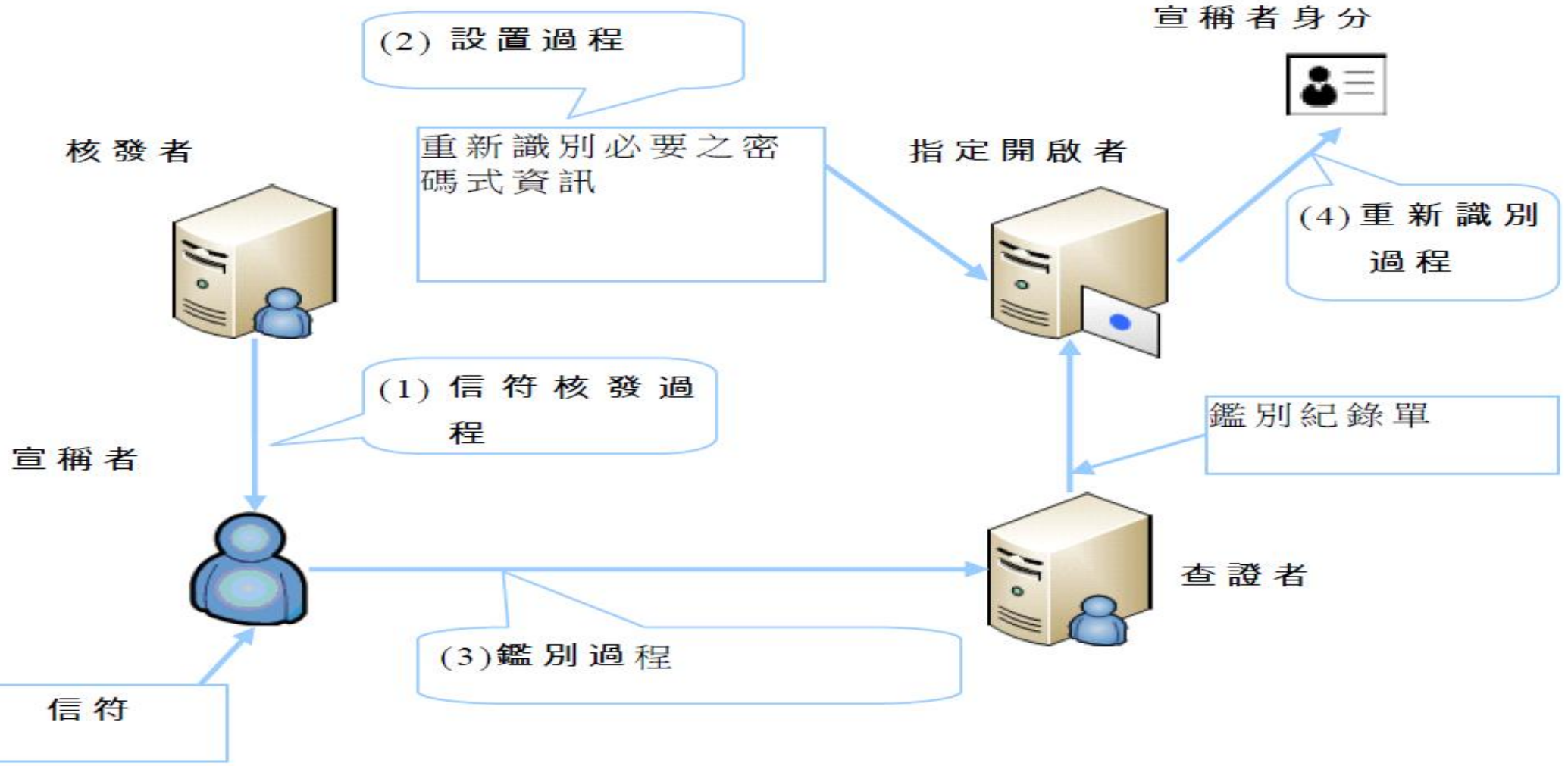
CNS 29100概念	CNS 27000概念
隱私權相關者	利害相關者
PII	資訊資產
隱私權違反	資訊安全事故
隱私控制措施	控制措施
隱私風險	風險
隱私風險管理	風險管理
隱私保全要求事項	控制目標

CNS 29191

- 資訊技術 - 安全技術 - 部分匿名及部分去連結鑑別之要求事項

- 通常傾向於將個體保持匿名及去連結
- 但於某些具正當理由之情況下，可後續啟動重新識別(例：確認可歸責性時)
- 〝部分匿名及部分去連結〞意謂事先指定開啟者，且僅該指定開啟者，可識別該鑑別之個體。
  - 例：圖書館可能需要識別未歸還所借書籍之個體，以便發送逾期通知予該個體。
  - 目前之密碼學技術可用以提供部分匿名及部分去連結之鑑別
- 此標準規定部分匿名及部分去連結鑑別之框架及其要求事項

部分匿名及部分去連結鑑別之框架



要求事項

(a)宣稱者應由查證者鑑別，而不能由查證者識別

- 對於向查證者保持匿名之宣稱者，其交易不應提供任何可用以識別宣稱者之資訊，但允許查證者證實宣稱者持有有效之信符

(b)鑑別紀錄單本身不得提供能連結同一宣稱者多項鑑別交易之資訊

- 對於向查證者保持不可連結之宣稱者，其交易不得提供可連結同一宣稱者履行之多項交易的任何資訊

(c)鑑別紀錄單應包含供指定開啟者重新識別宣稱者之必要資訊

- 為使指定開啟者之後能重新識別宣稱者，成功交易產生之紀錄單應提供識別宣稱者之資訊。注意，於適當情況下，指定開啟者可使用其他資訊以進行重新識別

(d)指定開啟者應能提供所宣稱身分為正確之證據

- 為避免指定開啟者之不誠實宣稱，指定開啟者應能提供重新識別程序已正當履行之證據

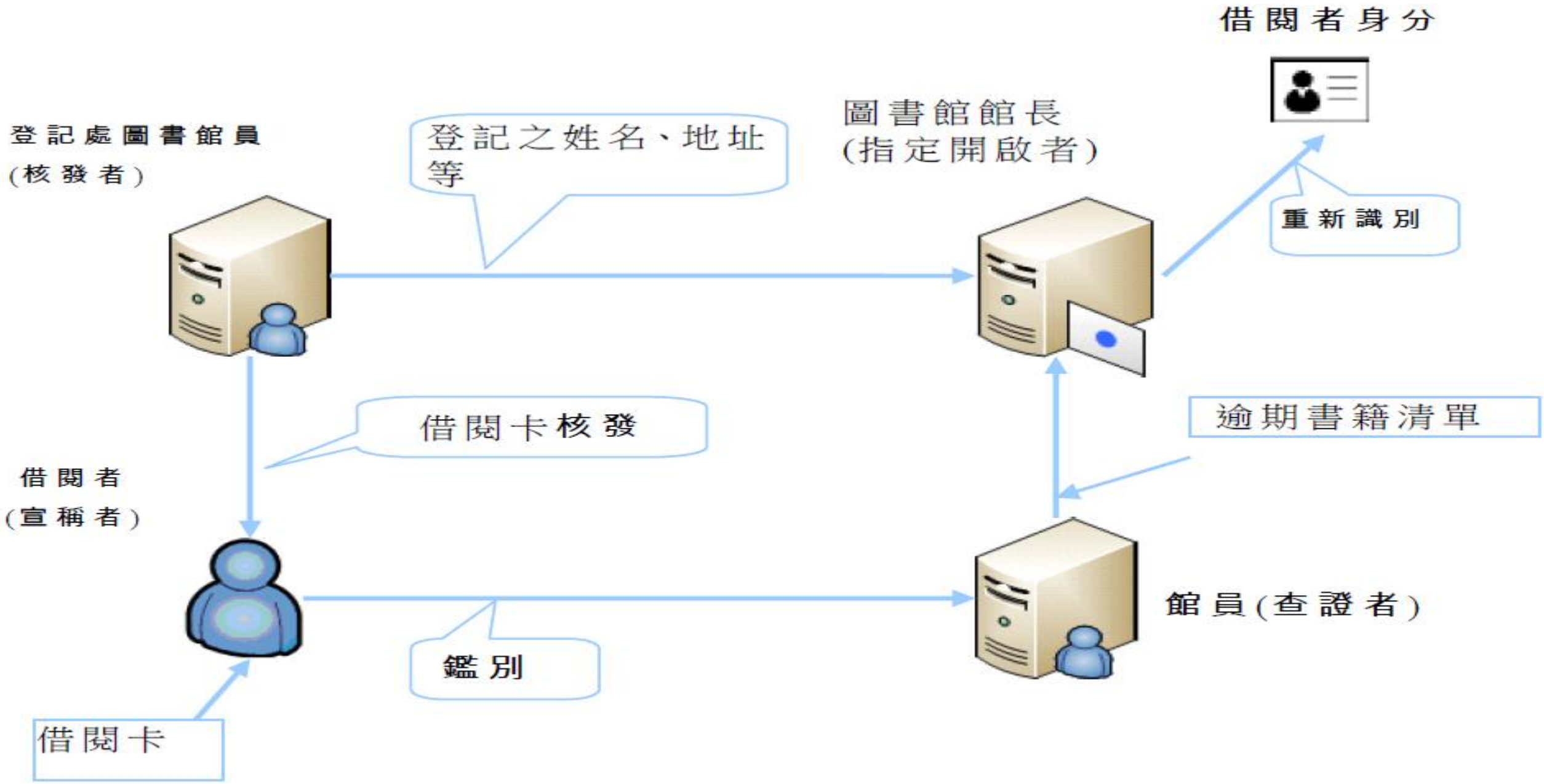

借閱者身分
登記處圖書館員
(核發者)
登記之姓名、地址等
圖書館館長
(指定開啟者)
重新識別
借閱卡核發
逾期書籍清單
借閱者
(宣稱者)
館員(查證者)
鑑別
借閱卡

圖 A.1　圖書館使用案例

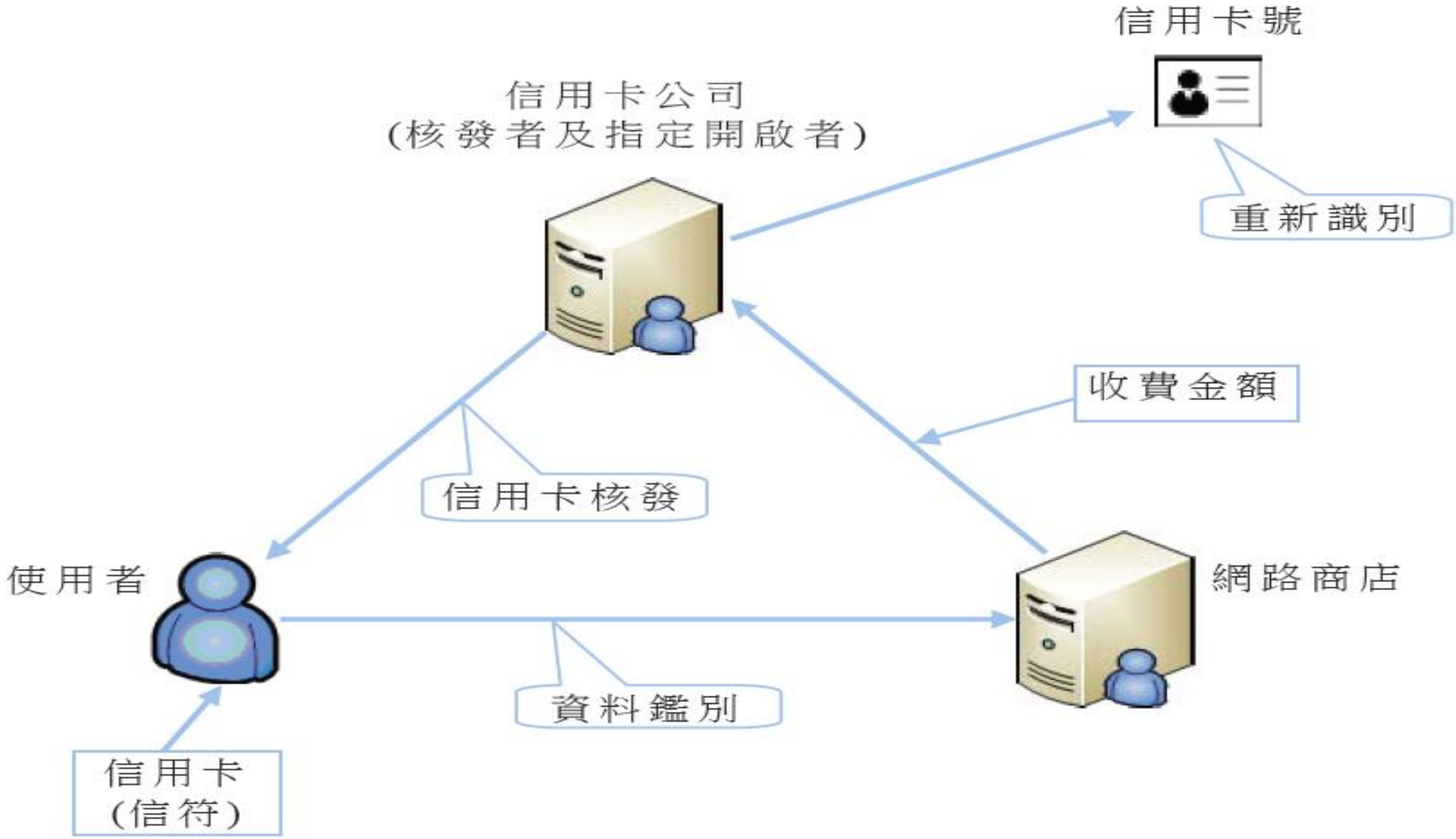


圖 B.1　隱藏付款帳戶

29191要求事項➔DID驗證要求事項

- **要求事項**：經匿名(或擬匿名)處理後資料之接收者應僅能鑑別個資當事人之資料屬性，而無法識別出個資當事人
- **要求事項**：同一個資當事人之經匿名(或擬匿名)處理後之不同資料，不得提供具有聚合後能連結至該個資當事人之資訊
- **要求事項**：資料經匿名(或擬匿名)處理後，應可由個資控制者重新識別個資當事人
- **要求事項**：個資控制者應提供能正確重新識別個資I當事人之證據

CNS 27018

- 資訊技術 - 安全技術 - 公有雲中PII處理者對個人可識別資訊(PII)之作業規範
- 對公共雲計算環境，依據CNS 29100之隱私原則，建立普遍接受之控制目標、控制措施及指導方針，供實作措施，用以保護PII
- 尤其是，規定依據CNS 27002之指導方針，同時考量對PII保護之法規要求(其可能適用於公共雲服務提供者之資訊安全風險環境全景內)
- 它適用於所有類型及規模之組織，包括公民營公司、政府機構，以及不以營利為目的之組織，其通過雲計算依據契約，以PII處理者為其他組織提供資訊處理服務。
- 指導方針亦可能與扮演PII控制者之組織有關；然而，PII控制者可能比PII處理者受到更多的PII保護之法律、法規及義務限制(此標準不規範)

- **Dropbox、Microsoft Azure已取得ISO/IEC 27018:2014驗證**

CNS 29101

- 資訊技術 - 安全技術 - 框架框架(*Privacy framework)*
- ISO/IEC 29101為維護隱私設置框架
  - 規定處理個人身份資訊之資通訊技術(ICT)系統的考量
  - 列出此等系統之實作組件
  - 提供此等系統置於全景中之架構概觀
- PII處理生命週期(PII processing life cycle)：包含PII之蒐集、移轉、使用、儲存、移除等階段

CNS 29134、29151之定位

Management system/framework

ISO/IEC 27001 : Information security management

ISO/IEC 29100 : Privacy framework

Risk management

ISO/IEC 27005 : Information security risk management

ISO/IEC 29134 : Privacy impact assessment

Controls

ISO/IEC 27002 : Code of practice for information security controls

ITU-T X.1058 | ISO/IEC 29151 : Code of practice for personally identifiable information protection

CNS 29151

- **個人可識別資訊保護之作業規範**
- CNS 27002+ CNS 29100
- 本標準為PII控制者提供廣泛範圍之資訊安全及PII保護的控制措施之指引
- 標準包含CNS 27002之指導綱要，並於必要時依據CNS 29100對此等指導綱要進行調整，以因應處理PII時所引起之隱私保護要求事項

CNS 29134

- **隱私衝擊評鑑之指導綱要**
- 隱私衝擊評鑑(PIA)係對處理個人可識別資訊(PII)之過程、資訊系統、計畫、軟體模組、裝置或其他行動方案等之隱私的潛在衝擊之評鑑工具，且於與利害相關者磋商後，採取必要措施以處理隱私風險的工具
- PIA不僅是工具：其係過程，開始於行動方案之最早階段，仍有機會影響其結果時，從而透過設計確保隱私。此過程持續直至專案部署完成，甚至之後
- 標準對下列各項提供指導綱要：
  - 隱私衝擊評鑑之過程
  - PIA報告之結構及內容

ISO/IEC 27701架構

- 4 groups of requirements:
  - PIMS requirements related to ISO 27001 are outlined in clause 5.
  - PIMS requirements related to ISO 27002 are outlined in clause 6.
  - PIMS guidance for PII Controllers are outlined in clause 7.
  - PIMS guidance for PII Processors are outlined in clause 8.
- Annexes:
  - Annex A lists all applicable controls for PII Controllers.
  - Annex B lists all applicable controls for PII Processors.
  - Annex C maps the provisions of ISO/IEC 27701 against ISO/IEC 29100.
  - Annex D maps the provisions of ISO/IEC 27701 against the General Data Protection Regulation (GDPR).
  - Annex E maps the provisions of ISO/IEC 27701 against ISO/IEC 27018 and ISO/IEC 29151.
  - Annex F provides guidance for applying ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002.

新PIMS驗證國家標準

- 29100-1資訊技術 - 安全技術 - 個資管理系統要求事項
- 依據我國個人資訊保護法及其施行細則、台灣個人資訊保護規範(TPIPAS)、2017年版BS 10012與CNS 29100
- PbD(Privacy by design, Privacy by default)
- 符合Annex SL MSS格式
- 已公告

法務部對個人資料去識別化之見解

個人資料之定義

- 依個人資料保護法第2條第1款規定，個人資料是指姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料
- 個資法將個人資料區分成兩類：
  - 直接識別之個人資料
  - 間接識別之個人資料

去識別化之定義 (引用法務部見解)

- 依個資法第2條第1款有關個人資料之定義反面解釋可知，所謂「去識別化」，即指透過一定程序的處理，使個人資料不再具有直接或間接識別性
- 如將公務機關或非公務機關保有之個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自無個資法之適用

去識別化過程

個人資料判斷之相對性

- 有關個人資料之定義對於個人資料或隱私之保護固然周全，但因得為比對組合之人及資料範圍具有「相對性」，故難有一致性之認定標準，如同個資法施行細則第3條修正理由說明所示：「是否得以直接或間接方式識別者，需從蒐集者本身個別加以判斷，此宜於個案中加以審認，...」
- 換言之，欲判斷一份資料是否為個人資料，對於不同蒐集者而言，即可能會產生不同之判斷結果，蓋蒐集者原先所持有或可能得以獲取之資料範圍有所不同，其與新蒐集之資料，是否得以透過對照、組合、連結等方式識別特定之個人，亦會有不同之結果，自難以一概而論

去識別化之行為定性

- 個人資料去識別化之行為應定性為個資法第2條第4款所稱之「處理」
- 而個資法之體系架構係將「蒐集」及「處理」行為規範於相同法定要件之下，蓋個人資料之「蒐集」大多緊密伴隨著「處理」行為，故個資法並未特別區隔兩者之行為要件，且因去識別化資料須達到無從直接或間接識別特定人之程度，故去識別化之加工處理並未增加對當事人權益之額外侵害
- 因此，如原先蒐集個人資料之行為符合個資法第15條及第19條第1項之規定，應可認為去識別化之處理並未逾越原先蒐集之特定目的（並非與原特定目的不相容），而得依據原先蒐集時之同一合法事由為之

函釋所稱「去識別化」範圍

- 如將公務機關保有之個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自非個資法之適用範圍
- 此後，公務機關主動公開或被動受理人民請求提供是類個人資料去識別化後之政府資訊，除考量有無其他特別法限制外，分別依檔案法第18條或政府資訊公開法第18條等相關規定決定是否公開或提供即可，無須再擔心是否符合個資法所規範之『特定目的內、外利用』的問題
- 「去識別化」，必須運用各種技術予以加工處理後，而依其呈現方式達到任何人（包含原資料保有者）無法運用一切合理可能之方法，透過資料比對或其他方式再直接或間接辨識出特定個人，此時該加工處理後之資料即非屬個人資料，而非個資法之適用範圍
- 函釋所稱之「去識別化」，必須達到前述「匿名化資料」或「不可逆之假名化資料」之程度，方得以全然排除個資法之適用

開放資料之去識別化程度

- 資料保有者於對外提供資料前，應進行整體風險影響評估，針對不同資料類型或資料提供方式，依比例原則分級控管去識別化程度
- 開放資料因係供不特定多數人自由使用該資料，並未限制資料提供之對象、使用目的或方法，而是以公開(publication)之方式提供，較難以控管其風險，因此對於所欲釋出之個人資料經加工處理後，自宜達「匿名化資料」或「不可逆之假名化資料」之程度較為妥適

加工匿名後無從識別之判斷標準

- 資料保有者須評估所釋出之去識別化資料有無合理之可能性，使資料接收者得與其他資料結合後而識別出特定個人，倘若釋出之資料本身雖不具有特定個人識別性，但如以此為線索，與其他已公開，或一般人可得獲取之「其他資訊」組合、比對下，亦得識別出特定個人時，則該釋出之資料將仍屬得間接識別之個人資料
- 從而，所謂「其他資訊」之範圍，自會影響去識別化之判斷準據

資料釋出者之責任(1/2)

- **刑事責任**：
  - 倘若資料釋出前業經多方風險評估及測試，且採取適當安全措施，並參酌資訊環境及技術發展等因素持續調整，而依當時科技或專業水準可合理期待重新識別之可能性已微乎其微，至少可認為已不具有違法利用個人資料之「故意」，而無個資法第41條之刑事責任
  - 又過失行為之處罰，以有特別規定者為限(刑法第12條第2項)，而個資法並無處罰過失行為之刑事責任規定。因此，應不構成刑事責任
- **行政責任**：
  - 個資法無特別規範，依人事相關法令處理，視具體個案有無人員行政疏失情事，再由該人員任職之機關進行後續懲處或懲戒

資料釋出者之責任(2/2)

- **公務機關國家賠償責任**：
  - 依個資法第28條第1項規定：「公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。」
  - 因此，倘若公務機關未善盡安全維護事項，致個人資料遭不法蒐集、處理利用或其他侵害當事人權利者，對於當事人須負「無過失之損害賠償責任」，無法以證明無過失之方式免責
  - 惟上開但書排除事變責任（第三人行為責任）及不可抗力責任，於具體個案，或許可主張所釋出之資料因已符合依當時科技或專業水準可合理期待之去識別化程度，被重新識別乃屬不可抗力、無法預見所致，從而依但書規定主張免負損害賠償責任，因目前缺乏具體個案，尚難預測法院見解為何

資料接收者進行重新識別個人資料之責任

- 依個資法第2條第3款之規定，所謂「蒐集」是指以任何方式取得可直接或間接識別特定自然人之個人資料
- 倘資料接收者嗣後卻運用特殊之技術或方法進行重新識別，進而取得個人資料，應可認為亦屬個人資料之「蒐集」行為，該資料接收者自仍須符合個資法有關蒐集、處理或利用之要件

個資去識別化驗證標準

緣起：個資利用疑慮

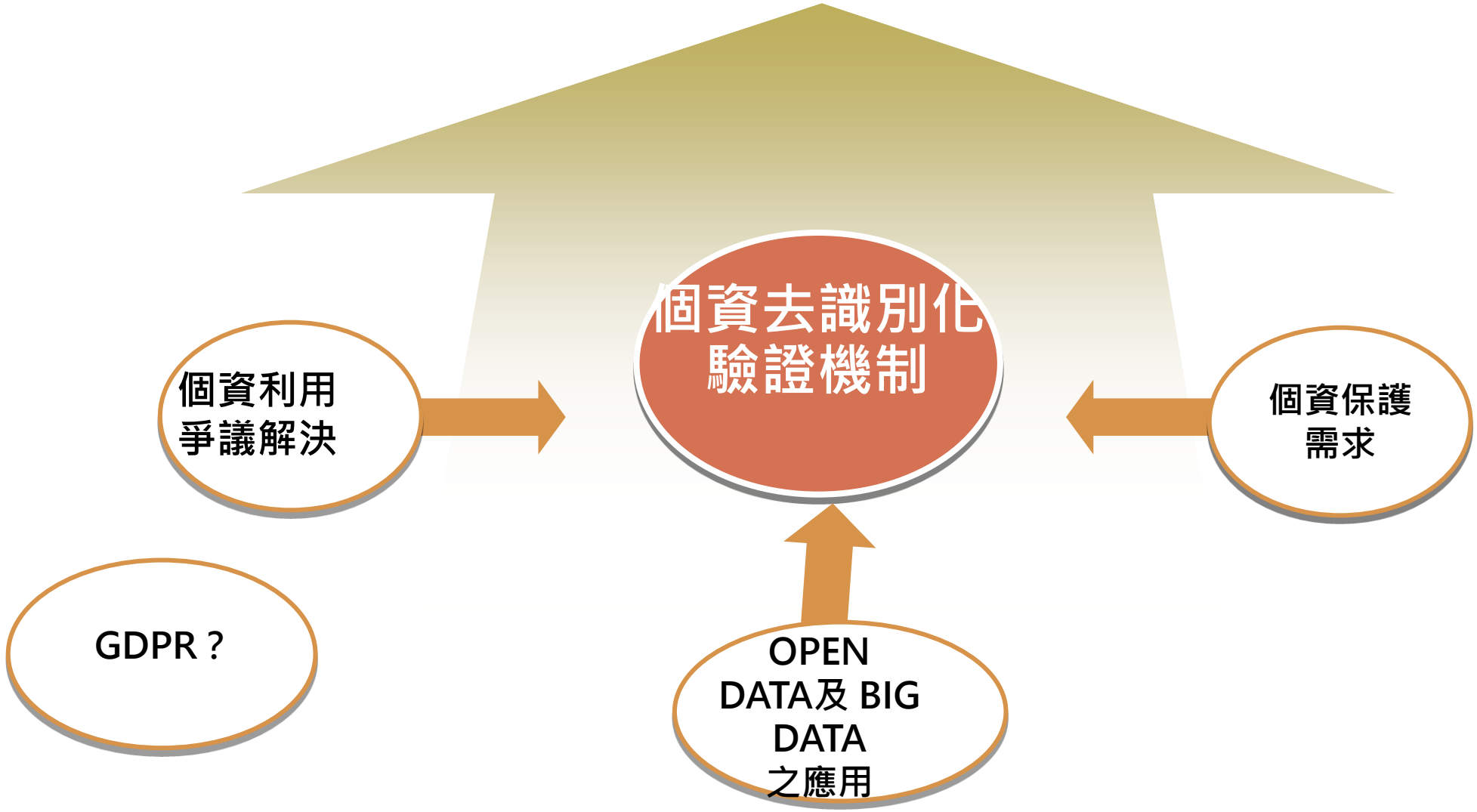
- 政府單位開放資料時，怕會洩露民眾個資
  - 衛福部健保資料應用之行政訴訟案
  - 公文書上滿紙OOXX...
- 民間業者希望能利用客戶資料分析，創造商機
  - 電信業者、第四台系統業者、電商業者

建立緣起：個資利用爭議

健保資料應用之行政訴訟案經過

- 101年2月媒體報導行政院擬打造「醫療雲」計畫，人權團體關注
- 101年5月4日7個民間團體召開記者會
  - ◆質疑健保局釋出健保資料給國衛院建置「全民健康保險研究資料庫」及衛福部建置「健康資料加值應用協作中心」與分中心作為學術或商業利用之法令授權依據
  - ◆後續健保局接獲26封存證信函，拒絕將個人健保資料供健保業務外利用，其中10人不服，提起訴願
- 101年11月衛生署駁回訴願
- 102年1月其中8人向高等行政法院提起行政訴訟
- 103年5月高等法院駁回
- 103年11月最高行政法院發回高等行政法院更審
- 104年1月高等法院召開準備程序
- 105年3月進行言詞辯論
- 105年5月高等行政法院駁回上訴
- 106年1月最高行政法院駁回上訴，定讞

個資去識別化驗證標準建立背景



歐盟去識別化技術意見書

◘ 歐盟去識別化技術(Anonymisation Techniques)意見書

– 2014年歐盟公佈去識別化技術意見書，評估不同去識別化技術，並提出資料達到去識別化的3項基本條件：

- 是否仍可唯一識別某個個人
- 是否仍可關聯到某個個人紀錄
- 是否能推斷出與某個個人有關的資訊

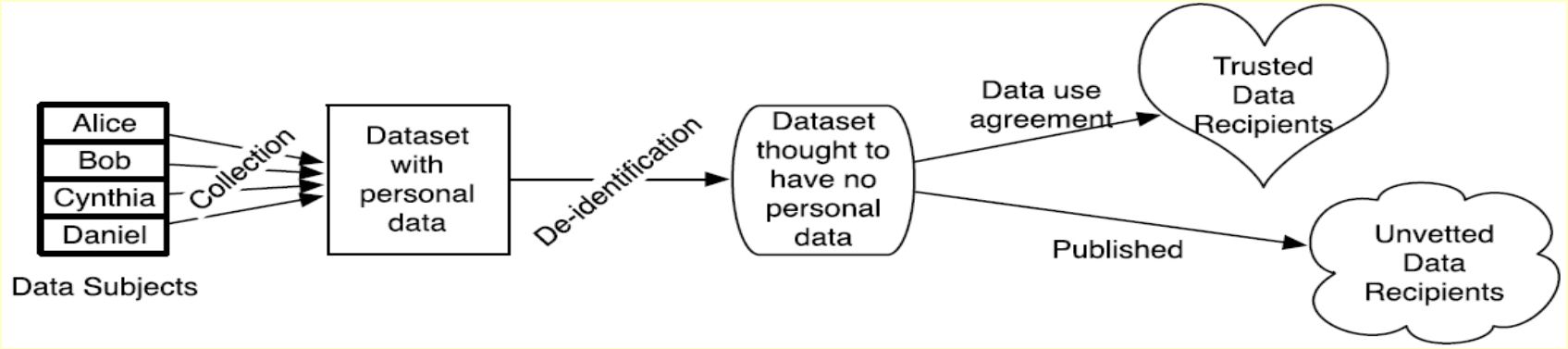
	是否仍然存在被挑出的風險？	是否仍然存在關聯風險？	是否仍然存在推論風險？
擬匿名化處理技術	是	是	是
添加雜訊	是	不太會	不太會
替換	是	是	不太會
聚合或K-匿名	否	是	是
L-多樣性	否	是	不太會
差分隱私	不太會	不太會	不太會
雜湊函數/憑證化	是	是	不太會

– 建議：

- 不採行“發佈後遺忘”，定期評估是否存在新的風險，重新識別（各種）剩餘風險
- 對於已確定的風險，評估已採取的措施是否足夠，並相應調整與持續監控風險
- 針對剩餘風險，特別考量非匿名化資料與匿名化資料組合時，是否會發生重新識別

美國個人資訊去識別化研究報告

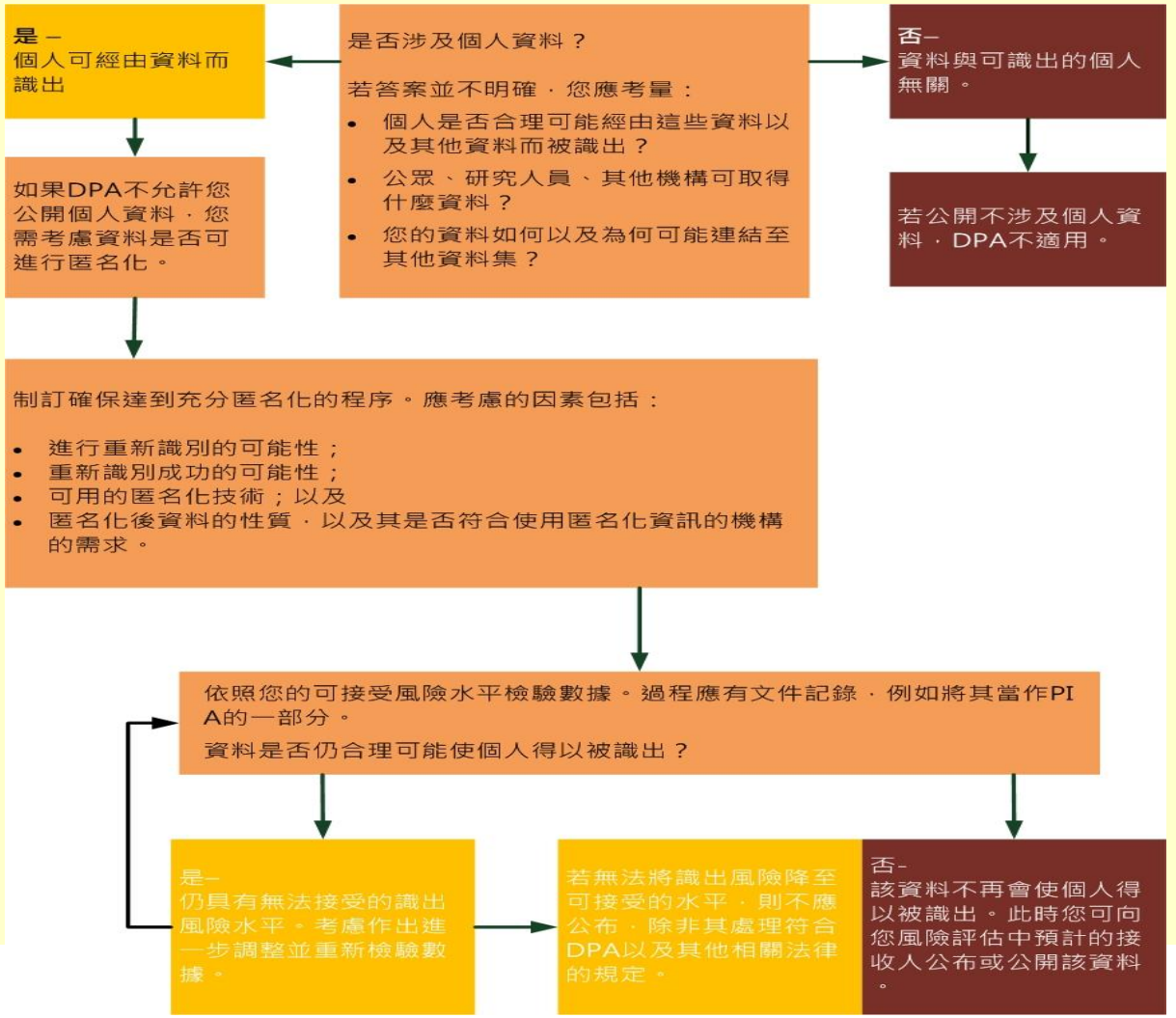
- **美國去識別化研究報告(**NIST IR 8053 De-Identification of Personal Information)
  - 隱私保護資料探勘：不釋出原始資料，加總或聚合之統計圖表。
  - 隱私保護資料：釋出經去識別化或聚合之原始資料。



- 資料釋出模式與控管：發佈後遺忘、資料使用協議、飛地（Enclave）
- 個資去識別化：
  - 移除直接識別資料，可參考美國醫療保險可攜性與責任法(HIPPA)定義之直接識別資料
  - 匿名化
  - HIPPA採取之去識別化方法：專家確定法、安全港法

英國去識別化實作作業規範

- 英國去識別化實作作業規範(ICO Anonymization: code of practice)
  - 作業規範僅提供良好的實作建議，本身不具強制法律效力，可供DPA規範所屬組織參考，亦可以使用不同的方法實作。
  - 個資開放流程：



ISO/IEC 20889

- **隱私增強資料去識別化術語與技術分類(Privacy enhancing data de-identification terminology and classification of techniques)**
- 提供有關隱私增強資料去識別化技術的描述，用以描述及設計依據CNS 29100中之隱私原則的去識別化措施
- 對表格化資料之已知去識別化技術進行分類，並描述其性質
- 特別根據去識別化技術特性規定術語、去識別化技術分類，並定義其用以降低重新識別風險之適用性

ISO 20889去識別技術分類

1. None
2. Pseudonymization with controlled re-identification
3. Pseudonymization
4. Masking of identifiers
5. Masking of outliers and selective quasi-identifiers
6. Generalization of selective quasi-identifiers
7. Randomization of selective quasi-identifiers
8. Implementation of K-anonymity for quasi-identifiers
9. Creation of synthetic data
10. Computation of statistics
11. Implementation of Differential Privacy server model
12. Implementation of Differential Privacy local model

去識別化過程驗證國家標準

- 29100-2 資訊技術 - 安全技術 - 個人資訊去識別化過程管理系統 - 要求事項
- 依據104年行政院公布之「個人資料去識別化過程驗證要求及控制措施」
- 已公告

個資去識別化標準結構及內容

- 遵循Annex SL 節次結構
- 用語及定義：依據 CNS 29100、CNS 29191
- 隱私政策：依據 CNS 29100之隱私政策，加上去識別化過程要求及資料分析過程要求
- 隱私風險管理過程：依據CNS 29100之隱私風險管理過程及 CNS/ISO 29134 PIA
- 去識別化過程要求：參考歐美相關規範
- 經去識別化資料之利用(資料分析過程)要求：參考歐美相關規範
- 重新識別要求：依據CNS 29191要求事項

資料去識別化後之重新識別風險計算

原則	解釋
重現性 (Replicability)	根據資料將持續連結至PII當事人之機率，將資料屬性定出風險等級之優先序。
資源可用性(Resource Availability)	判定哪些外部資源含有特定個人之識別資料及資訊中之重覆特徵，以及何人被允許存取該資源。
區別性(Distinguish)	判定某PII資料可於資料集之中被區別出的程度。
評鑑風險(Assess Risk)	必須同時綜合考量重現性、資源可用性及區別性風險。重現性風險、資源可用性風險及區別性風險越高，資料被識別出之風險越高。

驗證業務

- **驗證單位**
  - 目前有「台灣電子檢驗中心(ETC)」1家
    - 證書有效期限3年，每年需追查(follow-up)
  - 未來將有更多家加入
- **取得驗證證書單位(process based)**
  - 第一家財政部財政資訊中心「綜合所得稅核定資料」共720萬筆資料(於104年11月底取得)
  - 標準局、衛福部(多張)、國網中心、主計總處、
- **認證單位**：全國認證基金會(TAF)積極準備承擔此項工作，標準檢驗局將退出
- **輔導單位**：
  - 財政資訊中心係由工研院巨量資料中心與資策會科法所聯合輔導
  - KPMG、…
  - 未來會有更多家進入此產業

可能之驗證情境

- 依據法務部見解，將個人資料去識別化後之資料即不受個資法之約束
- 為因應「政府資料開放」及「巨量資料」之推動，需驗證各單位及公司之個人資料去識別化的過程是否妥善，以在可能之法庭個資訴訟中站在有利位置
- 許多政府單位及民間企業資訊能力不足，故資訊業務許多委外
  - 多數單位之個人資料去識別化驗證輔導將委外
    - 困難點在去識別化技術、PIA方法及風險估算方法
  - 個人資料去識別化業務(含重新識別之測試)可能委外
  - 定期重新識別之測試亦可能委外

謝謝聆聽
敬請指教