晶片國民身分證演進

--如何把國民身分證從紙本轉成晶片

中原大學資訊管理系兼任助理教授
潘國才

2024.3.28

四、個案研究方法 3 (歷史回顧研究,屬單一個案研究)

本頁簡報係引用宋教授餘俠授課講義

(一) 有一段時間 (二) 事實

(三) 有時間序列 (Time line) (四) 有一定知名度

(五) 以美國銀行資訊化成長變遷個案說明歷史回顧研究的七步驟

1. 問題聚焦：要能夠回答主要問題，X與Y要清楚
2. 定義範圍
3. 蒐集證據：擁護理論 (Espoused Theory) → 避免一廂情願

   資料來源主要來自於4種型式:

   (1) 書面型式 (2) 實體型式 (3) 傳聞軼事

   (4) 目擊證詞：非常重要 → 受限於事件的關鍵
4. 評論證據：驗證Ho就要否定Ha，需多角驗證。

   需找知名人士對研究加持 (權威的證言人)
5. 決定模式：深入感受與體會，藉此增進歷史紀錄的可信度。(同理心)
6. 陳述故事
7. 文字記錄

想要解決什麼問題？
（不見得都能解決）

1.定期更新身分證上的資料

2.加強身分證防偽技術

3.加強隱私保護

4.提高在網路上使用的便利性

5.提高資訊再利用的可能性

晶片國民身分證全面換發計畫

1 提案

1988年研議發國民卡 （國民身分健保合一智慧卡）政策引發社會爭議，隨後喊卡。

（2003年）健保卡全面 IC 化、發行自然人憑證

2015年10月內政部向行政院提報「晶片國民身分證全面換發計畫」，並納入2018年12月「智慧政府發展藍圖」中。

2 延遲與凍結

2020年7月，受疫情影響，全面換發時程延期。同年11月，立法院凍結預算。

3 暫停換發

2021年1月，行政院宣布暫停換發流程。

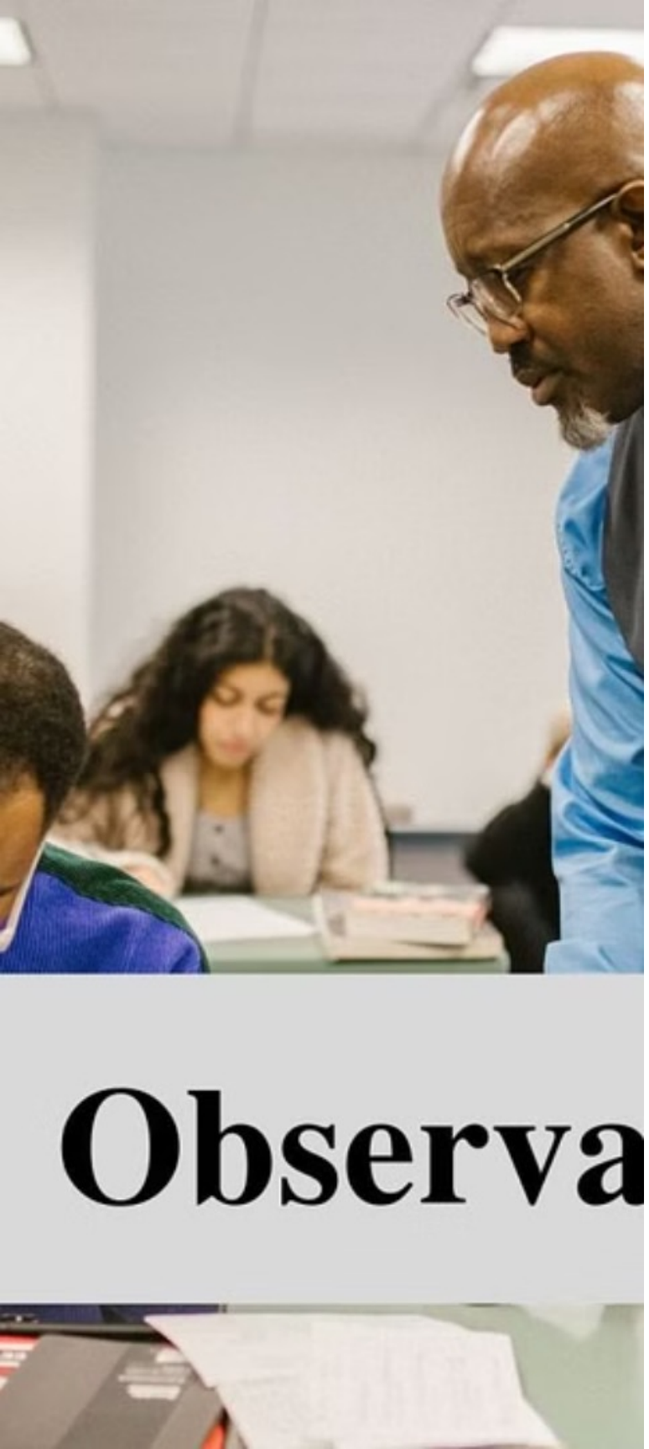
國外交流與學習

晶片證國際研討會

2017年7月，舉辦國際研討會邀請國外專家分享經驗。

與愛沙尼亞及德國

2017年7月，交流與愛沙尼亞及德國實務界專家、學者。



外界溝通

內政部

2017年2月，內政部邀請專家學者成立「晶片國民身分證換發專案工作小組」
2017年7月，內政部委託政大辦理「晶片國民身分證研討會」
2017年9月，內政部委託政大辦理「晶片國民身分證開放決策工作坊」

立法委員許毓仁

於2019年4月召開數位身分證(eID)公聽會，聆聽各界意見。

中研院政策建議書

於2020年11月提出建議，主張延緩換發流程。

規劃工程與進度(2019–2020)

0

國巨管理顧問公司

2019年4月得標「新一代國民身分證換發規劃案」。

1

東元電機得標

2020年2月得標PC晶片卡及印製設備乙式。

2

中華電信得標

2020年6月得標換發系統建置及維護案。

3

延期與混亂

2020年11月，立法院凍結2021年度預算4億元。

4

地方暫緩試辦

2020年12月，新竹市暫緩試辦新晶片身分證。

未來展望與挑戰

1 技術升級與應對疫情

需面對疫情對換發時程與技術進展的影響。

2 政策審慎與公眾需求

政府應審慎處理換發政策，並兼顧公眾需求。

科技與法律的交會

2013年	內政部附加自然人憑證研究
2019年4月	立法委員許毓仁召開數位身分證(eID)公聽會
2021年1月	暫停換發晶片證流程

身分與識別

- **身分**：足以代表一個「個體」資料，例如身分證字號、姓名等。
- [ISO/IEC24760 一組關聯到某個個體的屬性所組成的集合（A set of attributes related to an entity)]

- **身分識別**：經由一個設計的檢驗程序，確認個體與身分資料間的關係

身分識別程序

1.身分資料登錄

- 確認資料正確性
- 登錄於資料庫
- 掣發憑證（credential）

2.用憑證及符合驗證程序來確認身分

身分識別與身分驗證差異：問答題、是非題

參與單位	工作職掌
個體	身分識別的標的
信物服務提供單位（CSP）	負責管理信物生命週期以及個體與身分資料間關聯性的權責單位
註冊單位（RA）	負責登錄相關作業的權責單位
信賴單位	信賴並使用身分識別機制所得結果的單位
驗證單位（VA）	提供身分驗證服務的單位
公正第三方	除CSP、RA、VA所提供服務外，提供身分識別作業所需其他服務的單位，如身分核驗

3個程序

登錄

- 註冊
- 身分核驗

管理

- 信物管理
- 信物與個體關聯的管理

驗證

- 信物真偽
- 身分資料時效性確認
- 信物與個體關聯性驗證

網路識別機制介紹

1.自然人憑證（網路身分證）

2.健保卡（真的有身分識別功能嗎？）

3.金融卡

4.Mobile ID

5.FiDO

還需要晶片身分證嗎？

附錄

身分識別—要識別什麼（1/3）

來者何人（或公司或組織或設備）

奶奶：誰在敲門啊？　　大野狼：**我是小紅帽**　　奶奶：門沒鎖，推門進來吧

大野狼進門，把奶奶一口吞掉了

ISO/IEC 24760定義「身分」：

是由一組關於某個個體（entity）的「屬性（attribute）」所組成的集合

註：個體可以是自然人、法人組織、網站、伺服器、甚至是應用程式（ITU X1252）

問題：**「誰來決定身分」？**（繼續看下去）

身分識別—要識別什麼（2/3）

身分的決定（誰提供「身分」）

奶奶：誰在敲門啊？
大野狼：**我是小紅帽**
奶奶：門沒鎖，推門進來吧
大野狼進門，把奶奶一口吞掉了

奶奶心中：小紅帽是我孫女

如果大野狼回答：我是小矮人……

有權責的組織都可以在一定範圍內決定「身分」：

大家庭：阿公、阿嬤、爸爸、媽媽、伯伯、叔叔……
國家：國民身分證、駕照、護照……
公司：員工證、停車證、臨時人員證……
學校：學生證、教師證、職員證……
特定範圍：醫院就診證（現在各醫院都共用健保卡）……

身分識別—要識別什麼（3/3）

什麼是身分的驗證？

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

身分識別之書：連子清、杜宏毅合著(2022.3） P13

奶奶：誰在敲門啊？　　大野狼：**我是小紅帽**　　奶奶：門沒鎖，推門進來吧

身分驗證機制？？？　　奶奶心中驗證：小紅帽是我孫女

建立身分識別機制

身分可以被驗證先決條件

登錄：「個體」需先將身分資料登錄在某單位，要有下列三步驟：

1.登錄之前先進行確認個體

2.把與個體有關的資料登錄到資料庫中

3.設計一套機制，做為查驗身分資料時的憑據（credential），例如發出身分證、發出晶片卡或請建立一組通關密碼……或組合使用

查驗：對於「有身分驗證服務需求的單位」，必須遵守並信賴上述登錄身分資料單位所提供的驗證機制，所得查驗結果才有意義

身分識別之書：連子清、杜宏毅合著(2022.3） P14

建立身分識別機制

身分驗證機制中的角色

身分識別之書：連子清、杜宏毅合著(2022.3) P20

角色	工作	範例
個體（entity）	身分被識別標的	銀行客戶
註冊單位（Registration authority, RA)	負責登錄個體資料的單位	銀行的分行、戶政事務所等……
憑證服務提供單位（Credential Service Provider, CSP）	負責管理憑證（信物）生命週期以及個體與身分資料對應的單位	銀行資訊單位、內政部戶政司等……
信賴單位（Relying Party, RP），又被稱做需求單位	信賴機制查到的訊息並且使用該訊息的單位	其他銀行的付款設備、使用國民身分提供服務的單位
驗證單位（Validation Authority, VA）	提供身分驗證服務的單位	民間軟體憑證公司等
公正第三方（Trusted Thrid Party, TTP）	除CSP、RA、VA所提供服務項目外其他識別作業所需服務的單位，如身分核驗	內政部戶政司、醫院（嬰兒出生證明）

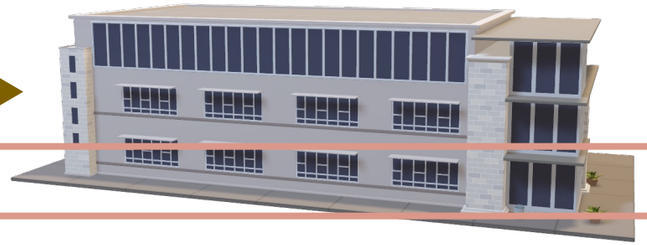
身分識別機制中各角色（1/2）

--以申辦國民身分證為例

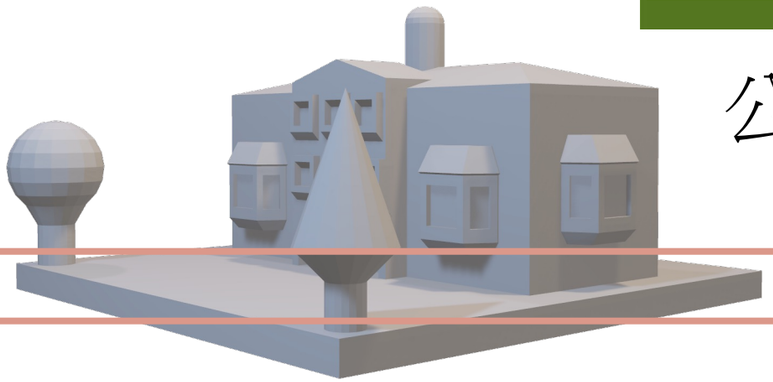
確認出生證明

申請

領證



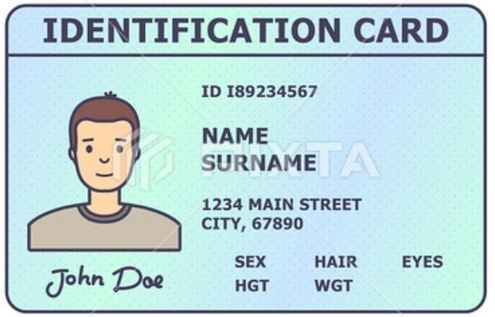
戶政事務所核驗身分（RA）



公正第三方（TTA）

戶政司登錄資料、製發憑證（RA）

申辦身分證（entity）

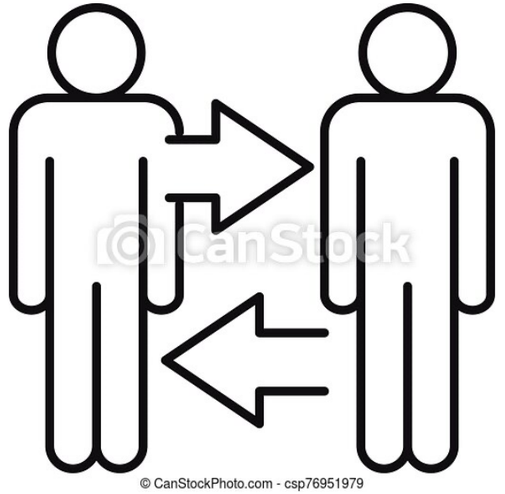


身分識別機制中各角色（2/2）

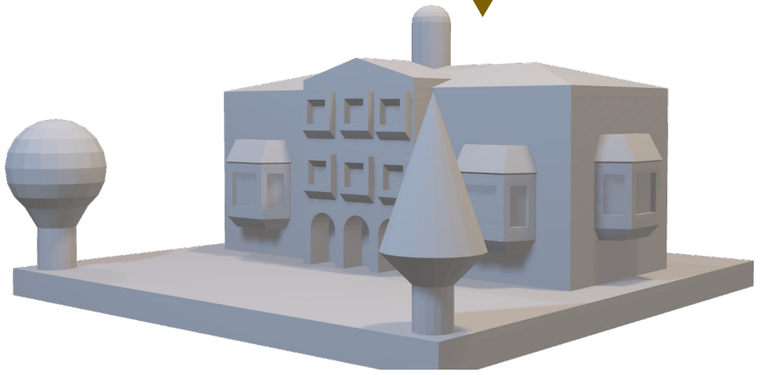
客戶要求服務

請出示憑證（RP）

軟體憑證



驗證單位提供驗證服務（VA）



憑證提供單位（CSP）確認憑證有效

網路身分識別機制分析（1/2）

網路身分識別可信度，有二大先決條件：

1.身分及資料管理嚴謹程度：包含確認個體、登錄、維護資料

2.多因子身分驗證（Multi-Factor Authentication, MFA)

透過各種方式檢驗下列因子

1.所具之形（something you are）
2.所知之事（something you know）
3.所持之物（something you have）

網路身分識別機制分析（2/2）

識別方法	特性	適用
帳密（ID + Password）	一般而言：身分管理由帳號發放單位核發，嚴謹度不高；驗證方式單憑密碼，屬於單因子驗證，無法確認輸入密碼者是否為具有身分者	非高風險系統中使用
一次性使用密碼（OTP）	強化密碼被盜用風險，但仍屬單因子驗證，驗證因子為「所持之物」（手機上的簡訊傳來密碼）。 如果查看手機上簡訊傳來密碼需要解鎖、刷臉、按指紋，則提升為雙因子驗證，增加了「所知之事」或「所具之形」	較帳密管控更高風險的系統
晶片卡	一般而言：身分確認機制較為嚴謹，屬雙因子驗證：「所持之物」（卡片）及使用時的密碼（所知之事）。	中高等級風險系統使用
PKI電子憑證	數位憑證及公私鑰組合成為「信物」，有嚴謹身分管理機制及查驗程序	可使用在高風險系統中
FIDO 註：PKI與FIDO差異比較可參考身分識別之書」	結合行動裝置上生物識別功能及密碼學上公私鑰演算法，因為在使用時使用「所持之物」或「所具之形」屬雙因子認證	可更便利使用在高風險系統中

網路身分識別機制設計原則

身分識別機制包含

1.登錄：確認「個體」與「憑證」（或稱為信物[credential]間關係
2.管理：憑證生命週期、有效性[ISO 29115 8.2]
3.驗證：以科技方式便利地確認個體所出示的憑證有效性，並回覆需求端。也同時要留存驗證記錄

設計身分識別機制，要

訂定管理政策機制、訂定落實服務品質機制、訂定風險評估以及信賴等級LoA評斷機制