數位皮夾設計規劃

用於認證與授權的分散式身分公共服務

版本：1.0.0

日期：2024.3.5

目錄

目標

本計畫預計將在民國 113 年（西元 2024 年），以公共程式（Public Code）為原則，發展並開放「數位皮夾」，使用者得以藉由授權、認證數位身分的過程實踐「個人身分自主權（Self-sovereign Identity, SSI）」，並逐步擴充功能。該服務將有效被各行動裝置、網路服務、身分發行者與數位服務提供商、web3 開發者有效介接，成為數位服務的基石，嵌入各特定服務之中。一方面加速各政府機關證件數位化進程，也同時協助民間身分發行者導入更安全、更容易互通的身分介接服務。民眾只需要使用這個服務，即可從各機關網站、各跨境平台、跨國事務與電子商務等管道介接不同數位身分，以簡單、安全、方便的方式，完成身分認證與授權功能。

本計畫的核心目標有三：

1. 打造兼具隱私與便利性的簽章與認證機制，強化資訊安全韌性。
2. 為政府各機關提供安全且便利的證件數位化解決方案，加速實踐智慧國家目標。
3. 建構可供跨境互認的身分介接協定，提升國人境外或數位生活的便利性。

描述

如同現實生活，人們可以將員工證、信用卡、集點卡、或任何一張足以識別其身分或屬性之卡片放進皮夾，數位生活也需要一個皮夾，用於「證明你是誰」與「讓你授權他人」等目的。公部門、私部門與個人都可以將所發行的憑證放進皮夾，這些證件可以是信箱帳號、學歷證書等公務用證件；也可以是會員卡、入場券等娛樂需求的兌換券。

「數位皮夾」是一個符合現代數位生活，用於日常數位生活的分散式身分系統，核心的兩項功能為認證（Authentication, AuthN）與授權（Authorization, AuthZ），本計畫藉由建置可供民眾自行決定收納臺灣各公私部門所發行之各式證件，來建構國人日常的事實身分（de facto identity），達到「個人身分自主，資料授權自決」目的。本服務為我國數位創新關鍵基礎建設計畫的一環，也是臺灣數位公共建設計畫。

對於證件或身分的發行者（Issuer）而言，「數位皮夾」初期將是一個軟體開發工具套件（Software Development Kit, SDK）與使用介面，協助任何身分的發行商，如政府數位憑證、企業金融憑證或一般人，介接已發行之數位憑證，並自動轉換成符合分散式身分識別符（Decentralized Identifiers, DIDs）與可驗證憑證（Verifiable Credentials, VCs）標準的「卡片」，存放在使用者（Holder）同意的「數位皮夾」中，這個過程為認證（AuthN）；而對

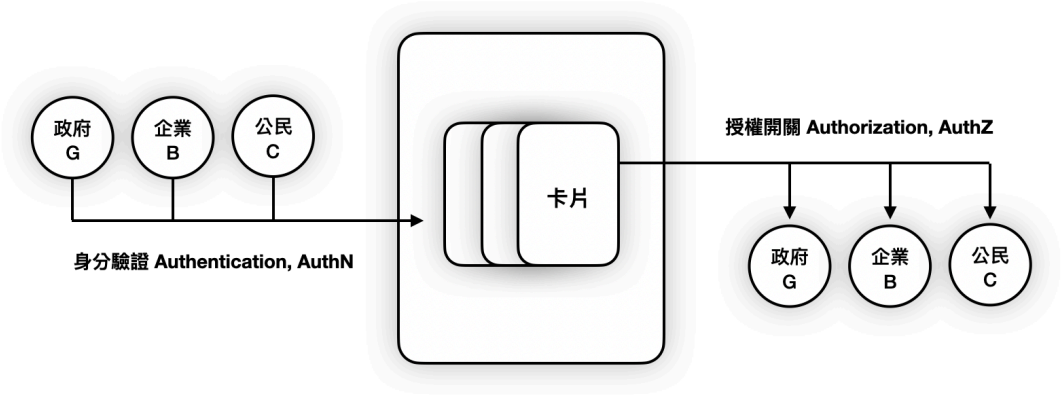
於使用者而言，「數位皮夾」則是一個操作介面、一個應用程式或數位服務，讓使用者可以依其需要儲存、展示、認證與授權其任一身分。

使用者可以自行決定是否開啟這些身分的授權功能，應用於外連服務，如簽章確認、企業活動或一般娛樂目的等，這個過程為授權（AuthZ）。授權過程符合隱私保護（Privacy Preserving）原則，並進行分層授權處理，降低透露不必要資訊的風險，此部份可透過如應用零知識證明（Zero Knowledge Proof, ZKP）或其他密碼學方式進行。相關授權功能由使用者個人自主管理，使用者隨時可以取消授權服務，此模式也因此稱為「授權開關」。使用者的授權開關背後的技術規格應可逐步介接任一符合互通標準的服務，如行動裝置提供的作業系統預設錢包、區塊鏈錢包服務或他國數位皮夾（digital identity wallet）等，並可根據使用者需求，介接相關安全服務，如密鑰管理等。而無論驗證者為何，如政府機關、企業服務或個人，只要經過使用者授權，皆可成為驗證者（Verifier）來驗證該名使用者所提供之資料是否為真。

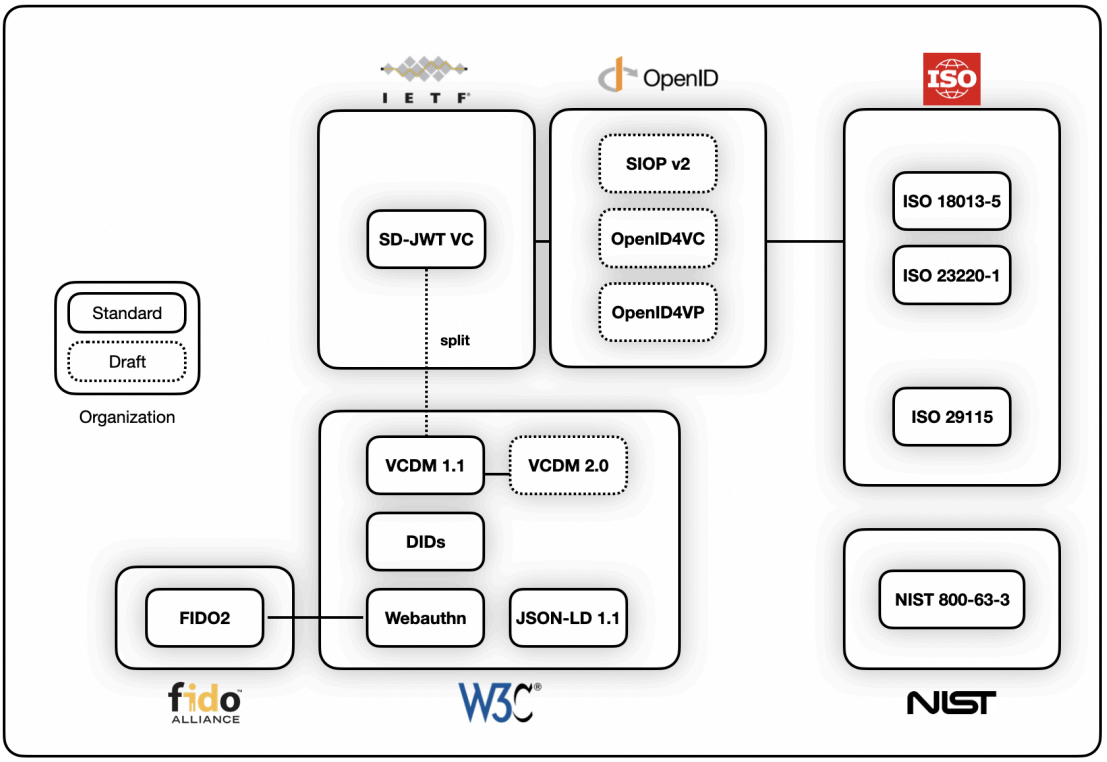
此外，如同現實生活中一個人可以擁有不只一個皮夾，在數位世界中，使用者也可以擁有多個「數位皮夾」，以區隔不同用途的身分憑證；使用者可以隨時從數位皮夾中撤銷這些憑證。

而為了有效建構「可組合、可跨境、非特許」的合作模式，上述分散式身分相關憑證將可被儲存在公共區塊鏈或分散式儲存系統中，讓這些經過隱私保護的憑證呈現可介接狀態，也供非特許之第三方進行驗證，進而促成跨境使用。本計畫將致力打造適合世界各地開發者複刻（fork）的數位皮夾，尤其是讓行動裝置服務、瀏覽器開發商與各國政府服務介接，並有效使用開發套件，讓臺灣所開發之數位皮夾可以被跨境應用。

「數位皮夾」以「優良保密協定」（Pretty Good Privacy, PGP）的非對稱式密碼學（Asymmetric Cryptography）之信任網（Web of Trust）精神運作、對應次世代之分散式識別符與可驗證憑證資料模型標準（W3C Decentralised Identifier, Verifiable Certificate Data Model）、《電子身分認證與信賴服務規章 2.0》（eIDAS 2.0）之歐盟數位身分錢包（EUDIW）與 web3 各數位身分服務等，建置國人新一世代身分連結與延伸服務的可信賴數位基礎建設，此部分可詳閱附錄二。



圖一、數位皮夾功能示意圖



圖二、相關標準盤點示意圖

特色

「數位皮夾」(分散式數位身分認證與授權系統)具有以下特色:

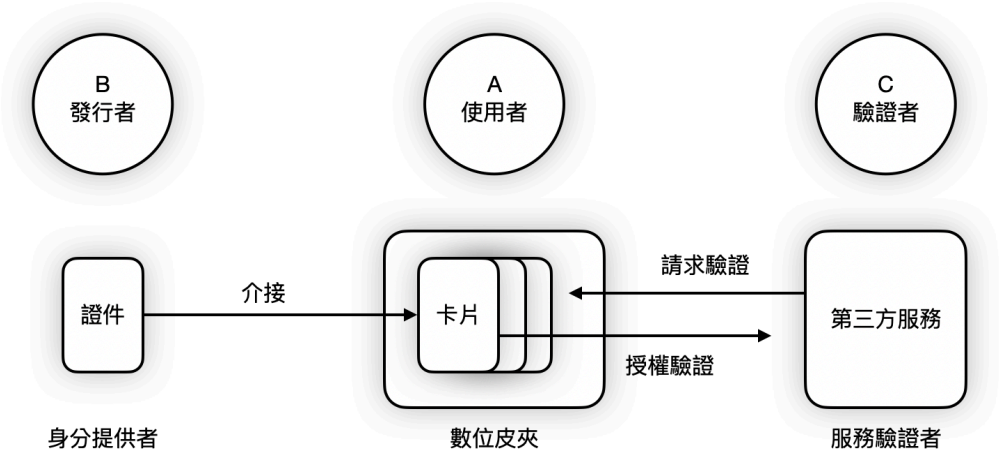
1. 事實身分(**de facto identity**):本計畫以「卡片」之組合,達成識別之功能。
2. 身分自主(**self-sovereign identity, SSI**):使用者隨時可取消或關閉介接之身分,亦即「總開關」之設計。
3. 社會關係可組合化、可程式化(**composable & programmable social relationship**),如可驗證展示標準(Verifiable Presentation,詳述見後)。
4. 非特許(**permissionless**)與開放原始碼(**open source**):亦即人人都可開發、導入、介接,無需政府許可。
5. 相容於跨境與次世代數位需求(**compatible with cross-border & future, e.g web3**),相關憑證加密存放於使用者裝置、公共區塊鏈或分散式儲存服務。
6. 無密碼(**passwordless**):使用生物辨識或硬體金鑰,得符合 FIDO 標準或多因子驗證相關標準。
7. 安全與隱私保護(**secure & privacy preserving**):符合最小揭露原則與公鑰密碼學機制方法,達到「次次登入皆須認證」、「次次授權皆有保護」的目標。
8. 功能等效(**functional equivalence**):符合本國與國際法規與協定。
9. 韌性與社會恢復(**resilience & social recovery**):整套系統避免單一伺服器故障風險。即使持證者的設備被竊,或伺服器所在機房遭摧毀,持證者依然可以快速地重新證明自己的身分。
10. 可選擇同意與可選擇退出(**opt-in & opt-out**):非強制使用,並遵守紙本使用權(**Protect a "right to paper"**)。

「數位皮夾」將遵守以下原則:

1. 不會發行新身分。
2. 不會於政府伺服器儲存生物辨識資料與私鑰,且該類資訊設計只儲存於使用者裝置中。
3. 不會作為以物件為主體的分散式身分,如貿易物件、數位交易物件等,但不排除於未來適合時,擴充與納入相容之可能性。
4. 在儲存使用者的個人資料前,均須獲得使用者的同意與授權。

關係人

本章描述各關係人使用本服務的情境。



圖三、服務需求說明圖

A. 使用者 Holder（或持證者）

1. 使用者為自然人、法人或非法人團體。
2. 使用者持有一個分散式識別符（DID）作為皮夾位址，接收其所欲存放之「卡片」。
3. 數位皮夾屬於數位公共基礎建設服務，以利於安全且方便的架構使用數位服務。
4. 使用者可自由登入各服務帳號，並以「卡片」方式儲存。
5. 面對新需求，使用者可以一鍵同意各「卡片」連結需求，但系統會給予警語。
6. 各「卡片」的連結狀態，將以卡片方式呈現，並陳列有連結需求的服務商，方便使用者管理。
7. 使用者隨時可以取消「卡片」身分或連結狀態（opt-out）。
8. 除了使用者授權之驗證者，其他人無法知道「卡片」由誰持有。
9. 獲得「卡片」之流程應比照現行服務設計。
10. 使用者可以生物辨識或硬體金鑰方式登入，無需記憶密碼。
11. 當使用者重複申請相同之「卡片」，先前的「卡片」將會自動失效（替換原則）。
12. 每一次在數位皮夾的授權，均需經過生物辨識或硬體金鑰，或根據信任層級啟動多因素驗證服務（MFA、相等或更優質之服務）。

B. 發行者 Issuer

1. 發行者可為政府機關、商業法人、外國機關或自然人個人，如
    1. 電信服務商，如 sim 卡身分或 mobileID；
    2. 數位服務身分提供商，如 Google ID、Line ID、TWID；
    3. 政府相關憑證發行機關，如 TW FidO。
2. 自然人可以發行「卡片」給其他自然人或法人。
3. 發行者可透過自己的服務（如既有身分供應商），讓使用者獲得新的「卡片」/ DID。
4. 每一張「卡片」只會對應到一個皮夾。
5. 每一張「卡片」均具生命週期之時效性，需要定期連結。
6. 發行者隨時可以取消所發行之「卡片」。
7. 發行者所發行之「卡片」，需由使用者自行決定（opt-in）是否將該卡片加入皮夾。
8. 發行「卡片」應比照現行服務辦理。
9. 發行者在發行前，應揭露資訊使其他驗證者知道何時、何地有互相連接的需求。
10. 發行者可提供轉移既有身分（IC 卡或非 IC 卡數位身分），或頒布新身分服務。
11. 各身分發行者有權撤銷「卡片」之有效性。

C. 驗證者 Verifier

1. 驗證者隨時可以開發與本服務互通的驗證功能。
2. 驗證者隨時可以請求使用者授權「卡片」認證，但卡片之「展示」（Presentation）須遵守最小揭露原則。
3. 驗證者有一套不同層級的認證建議清單與等級供相關服務使用者選擇。

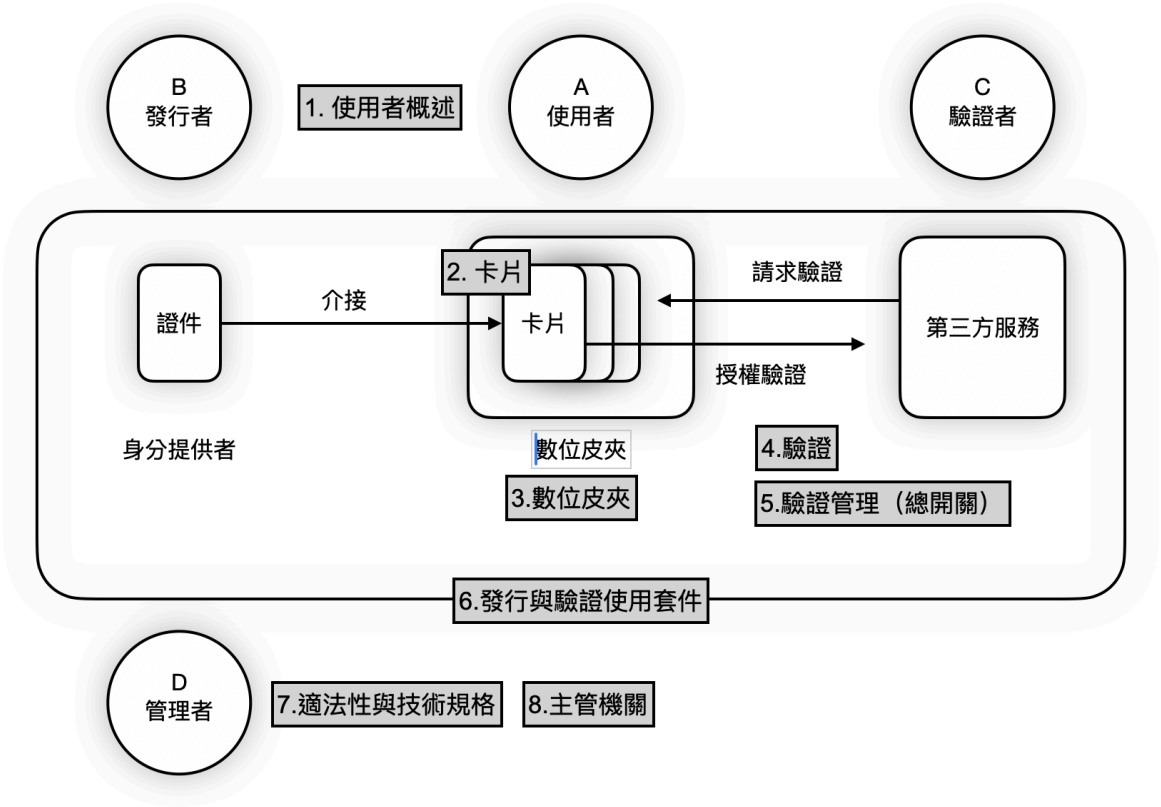
D. 管理者 Administrator

1. 官方版本的數位皮夾由數位發展部維護，且堅持公共程式理念，分享最新程式碼。
2. 數位發展部根據相關國際標準，建立驗證信賴等級（Authenticator Assurance Level，AAL）[1]建議清單，並建立經認證之發行者清單與對應申請辦法。

[1] NIST SP 800-63-3, NIST SP 800-63 Digital Identity Guidelines

服務需求說明

本章節描述各服務元件之定義與需求。



圖四、服務需求說明圖

0. 名詞解釋

- 驗證（Authentication, AuthN）：透過特定的方式，確認使用者具備某身分、擁有某卡片的過程。
- 授權（Authorization, AuthZ）：使用者（持有者）給予驗證者權限，允許其執行特定工作的過程。在本文中通常代表持證者將某些憑證連結至驗證者，使驗證者開啟或關閉某些服務。
- 使用者，或持證者（Holder）：申請使用數位皮夾的個人或組織。（見「使用者」章節）
- 發行者（Issuer）：發行並開放申請證件的個人或機構。申請過程中可能會記錄申請者的個人資訊。（見「發行者」章節）

- 驗證者（Verifier）：根據持證者展示之「卡片」組合，判斷持證者是否滿足資格的個人或組織。（見「驗證者」章節）
- 「卡片」：一種以符合分散式識別符（DID）與可驗證憑證（Verifiable Credential, VC）規格儲存，可供非特定第三方查證的可驗證憑證。其規格符合全球資訊網協會（W3C）所頒布之相關標準，並保留兼容後續其他標準之擴充性。
- 多因素驗證（Multi-Factor Authentication, MFA）：根據密碼等「所知之事」（Something You Know）、卡片與手機等「所持之物」（Something You Have）、生物特徵等「所具之形」（Something You Are）三類屬性確認身分的方法。涉及查驗錯誤會造成重大損失的中等信賴度（AAL2）以上之驗證作業時，均須至少同時驗證兩類因素。

1. 關係人概述

本節概述數位皮夾的整體功能。並敘述成為發行者、驗證者、持證者需要具備的條件，以及其分別需要擔負的責任。三個角色分別對應描述性需求盤點的三節。

1. 數位皮夾提供簡易的身分連結，使持證者能透過簡單地出示數位皮夾中的「卡片」，通過工作與生活中的各種查驗。

1.1. 卡片：以「數位皮夾」進行查驗的證件，源自可認證的數位憑證（VC）與分散式識別符（DID）。藉由符合資格之可互通協定或標準，「卡片」將記錄在「數位皮夾」中。

1.2. 持證者：無論國內外個人或團體，均可成為持證者。

1.2.1. 成為持證者無需申請。使用「數位皮夾」介接任一「卡片」之後，即成為當然持證者。（見「使用者」章節）

1.2.2.「數位皮夾」的保管，由持證者負責。

1.3. 發行者：除法律另有限制者外，國內外中央與地方政府部門、私人公司、非營利組織、非法人團體、以及自然人，均可發行「卡片」，成為發行者。（見「發行者」章節）

1.3.1. 成為發行者在技術上並不需要經過「許可」。

1.3.2. 發行者必須公開提出可申請「卡片」者的條件與規定，並寫明向其申請「卡片」時必須提供哪些資料與證明。（舉例來說，若要申請國際駕照證件，需要臨櫃辦理並進行認證；Google 帳號與相對應之證件須由 Gmail 信件驗證碼認證；然行動自然人憑證與數位皮夾對應之證件須通過 TW FidO 認證……）

1.3.3. 發行者發行的「卡片」，在資料規格上必須符合「數位皮夾」所設定之標準，包含 W3C DID 1.0 或 VCDM 1.1 Recommendation、eIDAS2.0、ISO/IEC 18013-5、ISO29115、NIST-SP800-63 等（詳見附錄二、數位皮夾標準盤點）。

1.3.4. 「卡片」發行之安全與驗證等級，必須符合使用地區之現行法規。

1.3.5. 發證時的檢驗相關資料與證明，由發行者負責。

1.3.6. 發行「卡片」所使用之金鑰對，由發行者負責保管。

1.3.6.1. 政府機關、金融機構等特許組織在使用智慧 IC 卡進行業務時，須遵守我國既有電子金鑰之相關保管規範，保管金鑰。應遵循政府機關公開金鑰基礎建設（GPKI）之架構為原則。

1.3.7. 持證者申請「卡片」時提供的資料保管，由發行者負責。發行者須遵守最小揭露原則，盡可能減少第三方能夠存取或得知之持證者屬性與資料。

1.3.8. 各司法管轄區均有驗證與授權的相關規定和技術標準。若「卡片」有國際使用需求，「卡片」與資料保管的標準，和針對該相應司法管轄區的法律遵循與相關責任，由發行者負責。（例如，歐盟的 GDPR 賦予使用者「被遺忘權」。發行者若要使「卡片」得以在歐盟使用，須設法使「卡片」與資料庫在功能上，能夠經過某些操作後永遠無法存取。）

1.4. 驗證者：除法律另有限制者外，無論國內外個人或團體，均可成為驗證者。（見「驗證者」章節）

1.4.1. 成為驗證者無需申請。

1.4.2. 驗證者可以根據希望持證者具備之屬性資訊（Attribute），如學經歷、財產、行動紀錄等等，列出認可的「卡片」列表。

1.4.3. 驗證者可以根據其需求，要求持證者授權單一「卡片」或是多張「卡片」，根據各「卡片」之間的邏輯關係，驗證持證者是否符合要求。

1.4.4. 驗證者可以根據「卡片」的授權，開放或關閉對應的數位服務。（例如社群平台判斷 A 帳號連結 B 單位發行之「卡片」，足供證實 A 帳號為自然人，因此給予 A 帳號藍勾勾。）

1.4.5. 驗證者必須根據發行者之信譽，以及「卡片」的驗證信賴層級（如 AAL1、AAL2、AAL3），決定是否認可「卡片」，並為後續影響負責。

1.5. 雙重性（**Duality**）：同一張「卡片」的發行者，也可以是驗證者。（如會員卡、社群平台，其本身管理身分系統，也提供數位服務。）

2.「卡片」

本節敘述「卡片」的檔案性質、能夠記載的資料、須具備的屬性或標籤。主要對應描述性需求盤點「發行者」一節。

2. 定義：「卡片」是一種儲存於數位皮夾，可供非特定第三方查驗的數位憑證，以可驗證憑證（VC）與分散式識別符（DID）規格儲存。它由發行者發行，介接在「數位皮夾」上，再授權至驗證者端。

2.1. 屬性（**Attribute**）：每張「卡片」所能證實的持證者屬性，由發行者決定。

舉例來說，有些「卡片」能證明申請者為自然人，有些「卡片」能證明申請者擁有某財產，有些「卡片」能證明申請者通過某考試，有些「卡片」能證明申請者加入某組織或某網站，有些「卡片」能證明申請者在某處買過飲料，有些「卡片」則單純能證明申請者可以進入特定安全層級的處所。

2.2. 屬性格式：「卡片」的資料規格，須含括工作與生活中所有查驗需求。包括但不限於：

- 身分證件
- 財產證明
- 服務證件如健保卡等
- 會員證
- 網站登入管道如帳號密碼等
- 入場券
- 消費證明
- 通知單
- 意願書
- 切結書

在資料格式上，這些查驗需求必須能夠由單一「卡片」滿足，同時必須能夠由多張「卡片」之間的邏輯關係滿足。

2.3. 必要屬性：「卡片」必須包含以下必要屬性，且屬性內容不得為空：

- 發行者
- 申請者
- 發證時間
- 有效期限

2.4. 發行者獨一性：「卡片」的資料格式，必須能夠確保發行者身分的獨一性。

2.5. 非必要屬性：「卡片」可以包含以下非必要標籤：

- 可供查驗的數值、字串

2.6. 有效期限：發行者在發行「卡片」時必須設定有效期限。「卡片」將在期限截止時自動失效（生命週期管理）。

2.6.1. 「卡片」必須根據發行者與持證者之間的協議，在有效期限截止前的設定時間，以「數位皮夾」、簡訊、Email 等方式，通知持證者重新申請。

2.6.2. 「卡片」須有自動停用的預設功能。當持證者的「卡片」一定時間內未介接至「數位皮夾」，或未授權至驗證者，「卡片」即自動停用，需要持證者另外啟用或展延。

2.7. 不可否認性（**Non-Repudiation**）：「卡片」在發行後，必須持續供申請者取用。「經官方認證」的發行者必須有一個介面，使申請者永遠都能查詢自己申請過哪些「卡片」，即使其中某些「卡片」已失效或已撤銷。這項特質將使每張「卡片」與 2.3. 所列的必要屬性，都不得更改，除經雙方同意後始得修改。

2.8. 存取控制（**Access Control**）：在正常環境下，只有發行者能發行「卡片」；只有發行者與持證者能撤銷「卡片」，其他人無法修改。

2.8.1. 例外狀況：當發行者或持證者違反我國法律，或者「卡片」的使用違反我國法律時，法定公部門可根據相應的法定程序，列出相關「卡片」不得通過的驗證，供驗證者遵循。參見「5. 驗證管理」與「7. 技術規格」相關條目。

3. 數位皮夾

本節敘述「數位皮夾」的要求、使用者的角色、使用方法；以及如何以「數位皮夾」操作「卡片」。主要對應描述性需求盤點「使用者」一節。

3. 定義：「數位皮夾」是一個供持證者使用的操作介面，得包括行動應用程式、數位服務、或其他方式。

3.1. 無需許可:「數位皮夾」無須註冊，下載安裝後即可啟用，亦得以數位服務的方式啟用。啟用過程無需申請任何許可，亦不驗證任何資料，這對發行者、持證者、驗證者皆然。

3.2. 無密碼（**Passwordless**）:「數位皮夾」採用無帳號密碼管理模式，並須符合 FIDO2/webauthn 等技術標準，包含生物辨識、行動裝置之密碼產生器、硬體金鑰等等，得以使用多裝置憑證（multi-device credential）或通行密鑰（Passkeys）等服務解決方案。

3.2.1. 多因素驗證（**Multi-Factor Authentication, MFA**）:「數位皮夾」必須具備「多因素驗證」功能。介接、啟用、暫停、切斷每張「卡片」時，均須啟動多因素驗證。驗證標準需符合相對應之驗證信賴等級（AAL）。

3.2.1.1.「數位皮夾」可透過生物辨識產生之私鑰、硬體金鑰或密碼產生器啟動各張「卡片」。

3.2.2. 私鑰自主:「數位皮夾」的私鑰與生物特徵，須符合相應資安標準，並僅儲存在持證者的手機等個人裝置中，或以使用者同意之方法保管密鑰，除此之外不得儲存在任何其他位置。（至於單一個人的不同裝置，如行動裝置、個人電腦或伺服器等等，可透過第三方 Passkeys 或其他標準規範等，經使用者同意使用。）

3.3. 鏈上公證（**Attestation**）:「數位皮夾」得在分散式伺服器或公共區塊鏈上讀取與寫入「卡片」的狀態，如申請、撤銷、身分連結、暫停使用、重新啟用等等。

3.3.1.「數位皮夾」操作「卡片」狀態的方式，服務提供者應納入「被遺忘權」（right to be forgotten）的考量。「經官方認證」的發行者須加入撤銷功能，使持證者能夠撤銷所指定之「卡片」與原身分之連結。

3.4. 多重持有:自然人、法人、或團體，均得以同時持有多個「數位皮夾」。

3.5. 保管責任:「數位皮夾」無需掛失，亦無需補發。裝載「數位皮夾」之裝置若不幸遺失，使用者僅需下載安裝新的皮夾，並向發行者重新介接各「卡片」，即能繼續使用各「卡片」之功能。相關「卡片」皆儲存在使用者端。遺失的「卡片」將於到期日失效，或於同一「卡片」重新申請時自動失效。裝置遺失時，若使用者擔心生物辨識或硬體金鑰之私鑰疑似被破解時，可聯繫各「卡片」之發行者撤銷（Revoke）之。

3.5.1. 使用「數位皮夾」的裝置遺失或刪除後，若須重啟服務，將由持有者重新申請、介接、綁定各「卡片」。

3.6. 替換原則：在預設條件下，一張對應自特定個人的「卡片」介接至新的「數位皮夾」後，即自動從其他所有「數位皮夾」切斷介接（亦即舊「數位皮夾」中的「卡片」將被撤銷）。

3.6.1. 例外狀況：在某些例外狀況下，一張「卡片」可以同時由多個「數位皮夾」介接。例如家長可以介接子女的健康保險「卡片」、看護者可以介接被看護者的健康保險「卡片」等，此例外許可由發行者端決定之。

3.7. 可互通性（**Interoperability**）：「數位皮夾」必須能夠介接根據相應規格發行之所有「卡片」，並標記自己目前持有這些「卡片」。

3.8. 可及性（**Accessibility**）與存取控制（**Access Control**）：「數位皮夾」必須有簡明的視覺化方式，供持證者啟用、暫時關閉、切斷各張「卡片」的連結。

3.8.1.「數位皮夾」必須顯示每張「卡片」的必要標籤，必要標籤列表見「2.3. 必要屬性」。

3.9. 最小揭露原則：每張「卡片」的非必要標籤，在「數位皮夾」介面中均預設為隱藏。這些標籤須經持證者授權操作後方能解鎖顯示，且僅顯示於使用者介接之「數位皮夾」中。

3.9.1.「數位皮夾」必須包含顯示標籤的 UI 功能，供使用者以翻面、額外點擊等方式，自行決定「卡片」標籤可顯示的範圍。

3.10. 隱私保護原則：「數位皮夾」送出的資訊，不得使持證者以外的任何一方，能夠辨別「數位皮夾」內每張「卡片」目前由誰介接，也必須符合「3.9. 最小揭露原則」。

4. 驗證

本節敘述以「數位皮夾」進行驗證的方式。主要對應描述性需求盤點「使用者」、「驗證者」二節。

4. 定義：每個「數位皮夾」能夠通過的驗證，均完全由「數位皮夾」所介接且已啟用之「卡片」所決定。

4.0.1. 中立性:「數位皮夾」不是憑證，也不整合任何憑證的資料。其本身沒有影響任一驗證是否通過的能力。

4.0.2. 分散:「數位皮夾」的驗證過程，完全由驗證者提出驗證請求，以及持證者授權「卡片」來完成。全程不需聯絡發行者，亦無需發行者主動參與，且不會透漏使用者的身分給發行者。

4.1. 待驗證項目:每個待驗證項都是一個符號邏輯(symbolic logic)算式。

4.1.1. 待驗證項必須完全由 AND、OR、NOT、EQV(等於)、>(大於)、<(小於)，以及各張「卡片」的代碼組成。(例如電商平台發行藍勾勾時，要求出示「至少 2 個跨境平台之會員證件」and「任一交易紀錄良好之金融帳戶」，此時可能的符號邏輯句為(〔abc > 2〕and〔xyz0001 or xyz0002 or ……〕。)

4.1.1.1. 可程式化(**Programmable**):驗證者可以用上述的符號邏輯算式，以及各張「卡片」所述之屬性，組合出能夠通過驗證的條件，藉此使證件的發放與驗證過程可自由組合、可程式化、分散程度大幅高於現狀，也使第三方使用者得以於安全前提下發揮創意，組合出更多潛在驗證場景，達到社會關係可程式化目標。

(範例 1:驗證「社群平台帳戶」 and「任何一張足茲證明為自然人之卡片」即可獲得真人驗證標章，如藍勾勾。)

(範例 2:經使用者同意，以匿名方式自主授權年度就醫次數等資料作為研究用途，達到資料募集目的。)

4.1.1.2. 可組合(**Composable**):可組合性能夠避免產生如目前集中式證件遭遇的問題。持證者的每項屬性可以分別由不同證件組合而成，不再需要集中在單一機構中，藉此降低單點故障的可能性，且達到社會關係可組合之現狀。

(舉例來說，任何一張足茲證明為自然人之卡片，可以與證明持證者具備財產的證件分開;證明持證者為合法駕駛的證件，也可以和其證明居住地的證件分開。)

4.2. 發出驗證請求:驗證者進行驗證時，將由驗證者介面送出待查驗的「卡片」符號邏輯算式，並要求「數位皮夾」回應。

4.3. 持證者授權:「數位皮夾」收到要求後，必須以視覺化的方式，依序顯示要求中的每個部份，分別可由哪些「卡片」來滿足，讓持證者依序選擇。

4.3.1. 如果驗證者要求的「卡片」條件，至少有一部分無法由「數位皮夾」內已介接的「卡片」滿足，則「數位皮夾」必須能夠在此時顯示，要通過驗證還缺哪類卡片所附帶之「相關資訊」。

4.3.2. 如果「數位皮夾」目前所介接的「卡片」中，有一張以上能夠符合驗證需求但尚未啟用，「數位皮夾」的介面必須能夠讓持證者決定是否啟用該張「卡片」。

4.3.3. 如果驗證者要求的「卡片」符號邏輯算式，足以使持證者授權之後透漏非必要之個人資訊，則「數位皮夾」此時必須發出警告。

舉例來說，登入線上購物網站時，「數位皮夾」可以先列出各張足茲證明為自然人之卡片」，供持證者選擇，再列出金融單位發行之「卡片」，供持證者選擇。

如果驗證者並非日常業務可被公信的組織，此時「數位皮夾」會跳出例如「這項查驗會讓對方知道您是自然人，且申請過 3 張以上信用卡。您確定要繼續查驗嗎？」的視窗，警告這項驗證可能透漏過多個人資訊，供持證者決定。

4.4. 回應驗證請求：「數位皮夾」將根據持證者的選擇，傳送相應的「卡片」部分資料供驗證者查驗，除此之外不可傳輸任何其他資訊，包括「卡片」記載之內容，或者該「數位皮夾」中介接的其他「卡片」列表，如 W3C 可驗證資料模型標準（Verifiable Credentials Data Model v1.1, VCDM）之可驗證展示（Verifiable Presentation, VP）[2]。

4.4.1. 查驗「卡片」的展示過程中，必須符合「3.9. 最小揭露原則」以及公鑰基礎建設方法。若有必要，得採用零知識證明（ZKP）等方式。

4.5. 連結「卡片」：驗證者查驗「數位皮夾」發出之「卡片」列表後，即將持證者選定之「卡片」連結至驗證者。

4.6. 通過驗證：「數位皮夾」提供的套件或應用程式，必須能讓驗證者簡單完成授權驗證過程。

[2] Verifiable Credentials Data Model v1.1: https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations

5. 驗證管理

本節敘述「驗證管理」，以存取控制權，加上「可驗證展示文件」（Verifiable Presentation）的生命週期，使持證者能夠獨立掌控卡片的「授權狀態」，是為「授權總開關」。

5. 定義：可驗證展示（VP）是一種經過加密編碼的展示，使驗證者在不看到原始憑證的前提下，依然能夠信任原始資料來源。
   5.0.1. 每次以「卡片」進行驗證的過程，都是一個可驗證展示。

5.1. 有效期限：每個「可驗證展示」均具有有效期限。
   5.1.1. 生命週期管理：憑證之展示必須設有時效，更新。該計時系統必須與發行者端「卡片」的有效時限系統同步。
   5.1.2. 數位皮夾系統須提供顯示介面，供持證者在授權驗證後，查詢該「可驗證展示」的有效期限。

5.2. 存取控制（總開關）：當持證者使用數位皮夾，暫停或中止「卡片」的啟用狀態，或切斷連結時，該「卡片」將無法列入下一次的「可驗證展示」。如果該數位皮夾內所有同類型「卡片」均被關閉或切斷，下一次的驗證就會失敗。

5.3. 充分告知與自主決定：在持證者改變「卡片」的啟用狀態時，數位皮夾必須讓持證者得以確認日後是否繼續接收該「卡片」的授權請求，是否重新申請或啟用該「卡片」並進行授權。同時也必須使持證者日後能夠修改這項決定。

5.4 充分自主掌握驗證授權歷程：持證者可查閱完整之驗證及授權歷程，驗證請求、請求日期、請求內容、授權情形、授權期間、授權範圍及時間戳記等資料持證者提供予驗證者查詢，並提供予驗證者查詢持證者，符合數位證據保存相關國際規定之「驗證授權卡片」。

6. 發行與驗證使用套件

本節敘述「數位皮夾」須開發的各種使用套件。這些套件能協助「數位皮夾」的驗證過程更順利進行，並供發行者、驗證者自行開發軟體與「數位皮夾」互動。主要對應描述性需求盤點「發行者」、「驗證者」二節。

6. 定義：「數位皮夾」必須提供一個或多個發行者、驗證者的使用套件、軟體開發工具套件，以及介接使用介面。

6.1. 發行者功能需求：此套件必須能夠使發行者得以根據相應標準，發行符合相應協定的「卡片」，供「數位皮夾」介接與操作。

6.1.1. 選擇同意（**Opt-in**）：這項套件必須允許發行者根據目前所持資料一次發行多張「卡片」，或在收到申請之後，逐張發行「卡片」。

6.1.2. 撤銷（**Revoke**）：這項套件必須能使發行者隨時暫停，以及隨時停用其發行的「卡片」，或使「卡片」失效。

6.1.3. 儲存與轉移：這項套件必須能夠相容未來的資料轉移需求與可能性，使發行者能夠根據相應標準建立轉移程序，根據既有的鏈上、線上或線下資料庫發行「卡片」。

6.1.4. 按需更新：這項套件必須讓發行者能夠根據最新的公私部門證件資料，如戶政資料、醫療資料、法律資料等，整批更新「卡片」的狀態。
（例如持證者失去行為能力或死亡時，相關「卡片」必須能夠及時撤銷。）

6.2. 驗證者功能需求：這項套件必須能夠使驗證者開發出查驗「卡片」條件，以及連結「卡片」的軟硬體與介面，符合相應協定，能夠對「數位皮夾」發出查驗請求，並根據「數位皮夾」提出的「可驗證展示」，給予服務。

6.2.1. 信賴需求：這項套件須對接「可信任服務清單」，以及驗證信賴等級建議，協助驗證者建立自己認可的「卡片」列表；並提醒驗證者在查驗這些「卡片」時，是否可能過度獲取持證者的個資。

6.2.2. 合規需求：這項套件必須得以使驗證者與公部門，能夠根據法定程序列出的禁／限用名單，自動暫停或終止相應「卡片」通過驗證的功能。禁／限用名單可能包括發行者、「卡片」、以及持證者。藉此保障持證者與驗證者之各種重要權利，並保障司法公權力能夠確實執行。

7. 技術規格

本節敘述「數位皮夾」與「卡片」必須符合的規格標準、資安標準。

7.1. 相容於 **web3** 需求：「數位皮夾」、「卡片」、與整套查驗系統，必須相容於 web3 之相應標準，並得相容歐盟 eIDAS2.0 與 EUDIW 等標準，確保使用者能夠以程式化的方式自由組合各種功能，拓展各種使用場景。

7.1.1. 因此，整套系統必須透過獨立的演算法進行，演算法必須具備抗審查性和韌性，並以分散式方式運作。

7.2. 獨立性:「數位皮夾」、「卡片」、與整套查驗系統，在規格上不得仰賴任一特定的軟硬體架構。

7.3. 等效性原則:各級「卡片」之適用範圍，由發行者認定，且需適用當地法規。

7.4. 資安標準:「數位皮夾」、「卡片」、與整套查驗系統，必須符合相應的資安標準。

8. 公部門管理單位

本節敘述「數位皮夾」與「卡片」的公部門管理單位，以及能夠獨立於發行者與持證者間操作「卡片」的組織。對應「管理者」一節。

8. 開放原始碼:「數位皮夾」、「卡片」、與整套查驗系統原則上均為開放原始碼之公共程式。相關原始碼在發布後即公開給所有人存取使用。

8.1. 維護單位:「數位皮夾」、「卡片」、與整套查驗系統的規格與版本，由管理單位負責維護與升級。

8.2. 發行者違法時之公部門管理單位:若因發行者違反當地法律，而必須暫停「卡片」之功能時，將由各法律規定之公部門管理單位，負責列出相應「卡片」名單，以及各「卡片」須暫停通過之驗證。

8.3. 持證者違法時之公部門管理單位:若因持證者違反我國法律，而必須暫停使用「卡片」時，將由各法律規定之公部門管理單位，負責列出必須暫停使用之持證者，或必須暫停使用之「卡片」名單。

結語

「數位皮夾」以新一代技術標準，提供了一套用於認證與授權的「身分」基礎建設，供各種有相關需求的個人、組織、團體，自行發行各種證件，同時根據各種證件決定給予何種服務。這能使驗證的內容跳脫目前集中式證件系統思維，回歸到每張證件分別能夠證明哪些屬性，以可組合、程式化的過程，建立一個分散式的驗證生態系。

數位皮夾基礎建設之目的，在於協助目前所有線上驗證、線上登錄、實體文書驗證，以及絕大多數的物理驗證管道，能夠更加迅速與便捷。

此外，由於這個生態系的證件類型與驗證條件，都比既有的驗證方式更多元，這個生態系將可創造目前難以實現的驗證場景。

最重要的是，數位皮夾的規格設計，盡可能減少了驗證過程中的個資露出，達到「最小揭露原則」，也同時盡可能的減少了登入時的帳號與密碼需求，符合「無密碼驗證」的資安發展趨勢。同時，它將授權所需的驗證程式化，並創造「可組合」的授權條件，社會將不再需要為了發行任一權威證件，而將大量敏感個資交給任何一個組織，大幅降低單一資料庫被入侵或濫用的風險。

可組合、程式化特性能有效緩解數位監控、資料洩漏、資料濫用的威脅，比既有的驗證方式更能維護資訊安全與數位人權。另一方面，這套驗證系統也能進一步降低身分證件的集中程度，降低單點故障的可能性，落實身分的自主性與韌性。

目前已有 EU Digital Identity（EUDI）Wallet、Polygon ID、Microsoft Entra 等多個組織，正各自在推廣、實驗與實踐這項目標。我國身為數位科技與數位民主的先進國家，應該在技術規格、生態系發展、推廣程度上維持最前線，確保相關科技產業的發展潛力與國際吸引力；同時確保我國未來的身分驗證方式，能夠盡量與其他國際民主社會的公私組織跨境互通，達到全民夥伴關係（People-first Public Private Partnership）。

附錄一、分散式身分原則需求盤點

我國「數位皮夾」之設計原則，與全球資訊網協會（W3C）公布之分散式標識符用例和需求（Use Cases and Requirements for Decentralized Identifiers）[3]草稿（Draft Note）有許多呼應之處。該文件列出 22 項 DID 需求：

1. 身分驗證/控制證明：可以證明 DID 的持證者是本人。
2. 分散/自主發行：DID 的控制權與發行權完全掌握在持證者（同時也可能是 DID 代表的對象）手中，不會轉移或分割到驗證者身上。驗證者毋須負責 DID 的發行、更新、復原，只需要用 DID 來識別、認證、授權即可。
3. 獨一無二：每張 DID 都是獨一無二的，不會重複。
4. 無需聯絡發行者：無需聯絡發行者，僅需使用 DID 即可完成驗證。
5. 以加密方式確保控制權：以緊密結合的加密材料，確保 DID 的控制權始終掌握在持證者手中。
6. 簡易的金鑰更新：需要更新身分驗證的材料時，無需發行者手動干預，DID 的金鑰即可更新；且過程中盡量不需要真人確認。
7. 尋找服務端點：驗證者可以自行搜尋可用的服務端點，與 DID 所代表的對象互動。
8. 隱私保護：使用 DID 不會洩露 DID 代表對象的任何資訊。
9. 控制權委託：持證者可以將 DID 的控制權委託給第三方。
10. 跨管轄：DID 的真實性與可靠程度，與它們在哪個司法管轄區發行無關。它在所有管轄區同樣適用，沒有任何一個司法管轄區能夠直接阻止人們使用 DID。
11. 行政機關無法否認：行政機關無法刪除或否認 DID 的存在。即使政權轉移或有心人士刻意干預，DID 仍屹立不搖。
12. 使用費盡量低廉：DID 不按照使用次數收費。未使用時沒有維持費用。因更新而產生的費用（因為網路費用、運算成本等等）必須「微乎其微」。
13. 不受供應商壟斷影響：DID 無需仰賴任一供應商，藉此避免供應商將 DID 的使用範圍限制在特定範圍內，並藉此收取不成比例的抽成。
14. 反追蹤：無論是 Cookie 這類目前的 session/state-tracking 機制，還是各種新的資料通訊系統，都可能被用來追蹤數位足跡。DID 系統必須能夠抵抗這種追蹤。
15. 相容於未來的加密科技：DID 能夠隨著技術的發展而更新。量子電腦能夠輕易破解目前的加密技術。DID 必須能夠相容於未來的科技，在新的身分驗證和授權科技下，繼續沿用相同的 DID。

[3] https://www.w3.org/TR/did-use-cases/#requirements

16. 不擔心發行者消失：無論發行者倒閉、被收購（可能失去網域或根憑證）、名存實亡無法繼續驗證過去發行的憑證是否為真，DID 都必須繼續存在。
17. 不擔心驗證者系統過期：即使驗證者的系統過期，DID 也安然無損，可以從當下的系統無縫接軌到下一代的新系統。
18. 不仰賴服務供應商：持證者與服務供應商之間的關係，不會影響到 DID 能否使用。DID 不會像郵件地址那樣，因為服務供應商消失，或者使用者不再使用供應商，而無法繼續用來進行驗證。
19. 加密認證和通信：用加密技術驗證個人身分，並以公鑰—私鑰之類的方式，保障 DID 代表對象的通訊安全。
20. 不綁定登錄格式：所有採用相容格式的登錄檔，都可以用來發行 DID。不依賴任何特定登錄技術或特定供應商。
21. 合法身分：DID 可用作憑證和交易的基礎，在一個或多個司法管轄區下被視為合法有效。
22. 人本互通性：即使不懂科技、沒有相關專業知識的人，也可以輕易使用。

將這 22 項需求與「數位皮夾」之設計原則相比較，可知我國「數位皮夾」之設計大多數符合，並在其中數項需求具備獨特優勢：

表一 DID 原則與需求盤點

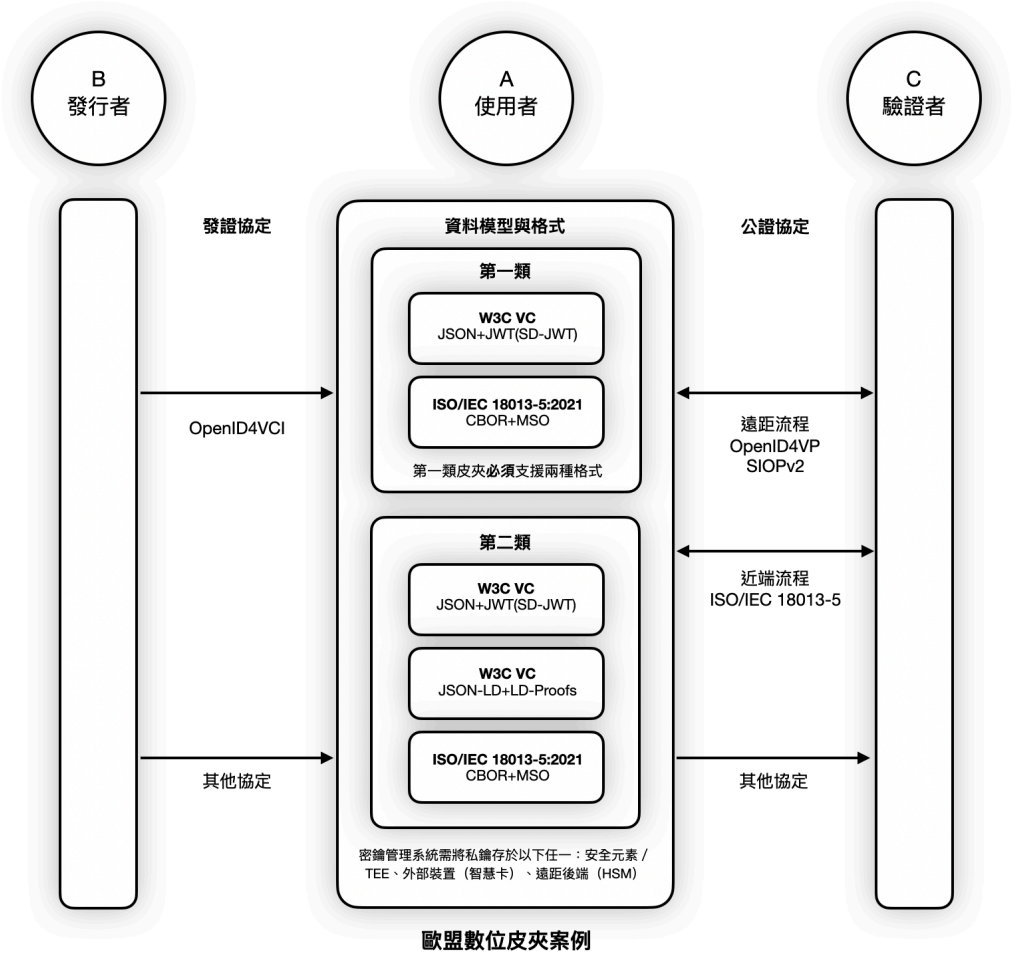
	1 事實身分	2 身分自主	3 社會關係可組合化	4 非特許與開放原始碼	5 相容於跨境需求	6 無密碼	7 安全與隱私保護	8 功能等效	9 韌性與社會恢復
1		◎				⊙	◎	⊙	⊙
2		◉	◉		⊙	⊙			⊙
3					⊙	⊙	⊙		
4	◎		◉						
5					⊙		⊙		
6	◉		◉						
7	◉		◉	⊙					
8	⊙	⊙	◎			⊙			
9	X	X	X	X	X	X	X	X	X
10			◎	◎	⊙			⊙	
11	◎	◎	◎	◎	⊙			⊙	◎
12	-	-	-	-	-	-	-	-	-
13	⊙			◎	⊙	◎			
14	⊙	⊙	⊙			⊙	⊙		
15	-	-	-	-	-	-	-	-	-
16	⊙		◎	⊙	⊙	◎			◎
17	⊙	⊙	◎		⊙				⊙
18		⊙	◎			◎			◎
19					◎	◎	◎		
20	◎		⊙	⊙					⊙
21	⊙							◎	◎
22		◎		⊙		⊙			
表例說明:◉ 高度相符;◎ 中度相符;⊙ 相符;X 互斥;- 未包含									

附錄二、數位皮夾標準盤點

1. 歐盟數位身分皮夾架構參考框架

本段落整理自歐盟網路安全局（The European Union Agency for Cybersecurity, ENISA）出版「數位身分標準」[4] 與歐盟數位身分皮夾（EUDIW, the European Digital Identity Wallet）之第一版「架構參考框架（ARF, architecture and reference framework）」[5], 作為我國「數位皮夾」標準參考及未來比較盤點, 以期望相容於跨域需求, 拓展各種使用情境。

歐盟數位身分皮夾將其標準需求分為兩類型, 本段補充主要聚焦於類型 1 的相關規範: 類型 1 聚焦於個人識別資料（PID, Personal Identification Data）, 為符合 ISO 29115高度信賴等級（LoA3 ）使用案例, 以實現跨境識別。



圖五 歐盟數位皮夾標準案例（重製）

[4] Digital Identity Standards, 來源：https://www.enisa.europa.eu/publications/digital-identity-standards
[5] EU Digital Identity Wallet Architecture and Reference Framework，來源：https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md

必須達到的規範包含但不限於：

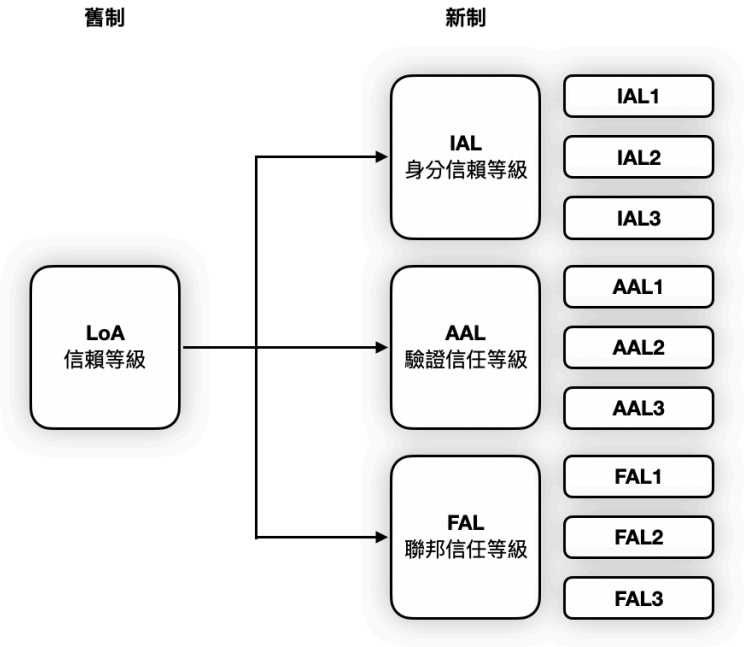
1. 密碼鑰匙管理系統（**Cryptographic keys management system**）
    a. EUDIW 方案必須依賴以下幾種組件之一來儲存和管理密碼鑰匙：
        i. 嵌入式安全元件或可信任執行環境（TEE，Trusted Execution Environment 適用於移動設備），
        ii. 依賴外部裝置（安全元件 / IC 卡片），以及
        iii. 後端（遠端硬體安全模組）。
        欲選擇哪種安全硬體以及支援哪種，取決於各個 EUDIW 方案。
    b. EUDIW 方案必須實作安全措施以防止密碼學洩漏風險。
2. 證明交換（**Attestation exchange**）
    a. EUDIW 方案必須支援 OpenID4VP 作為遠端操作流程的證明交換協議。當需要匿名身分驗證時，發送請求的參數應按照 OpenID SIOPv2 協議指定。
    b. EUDIW 方案必須支援 ISO/IEC 18013-5:2021 標準中詳細說明的協議，用於近距離操作流程。
    c. EUDIW 方案必須能夠執行擁有證明（proof of possession）。
    d. EUDIW 方案必須支援 ISO/IEC 18013-5:2021 標準中指定的屬性選擇性披露（Selective Disclosure）。
    e. EUDIW 方案必須支援 SD-JWT 標準中指定的屬性選擇性披露。
3. 發行協議（**Issuance Protocol**）
    a. EUDIW 方案必須支援 OpenID4VCI 作為發行協議。會員國可在其國家解決方案中自由包含額外的發行協議選項。
4. 資料規範（**Data model**）
    a. EUDIW 方案必須支援按照 ISO/IEC 18013-5:2021 標準指定的資料規範發行的證明。
    b. EUDIW 方案必須支援按照 W3C 可驗證憑證資料規範 1.1 指定的資料規範發行的證明。
5. **PID** 和 **(Q)EAA** 格式（**PID & (Q)EAA formats** ）
    a. EUDIW 方案必須支援 JWT 和 SD-JWT 格式的證明。
    b. EUDIW 方案必須支援 CBOR 格式的證明。
6. 簽署格式（**Signature formats** ）
    a. EUDIW 方案必須支援符合 JOSE（JWT）規範的簽署和加密格式。
    b. EUDIW 方案必須支援符合 COSE 規範的簽署和加密格式。
7. 密碼套件和機制（**Cryptographic suites and mechanisms** ）
    a. EUDIW 方案必須支援用於 SOG-IS 同意的密碼機制版本 1.2 中詳細的屬性的密碼套件和機制。

2. 信賴等級（LoA）與 XAL[6]

美國國家標準與技術研究院（NIST，National Institute of Standards and Technology）對數位身分服務的聯邦機構提出了技術要求。NIST 800-63-3《數位身分指南》擴展了最初在 Office of Management and Budget（OMB）Memorandum M-04-04 及ISO/IEC 29115 [7] 中規範的數位身分電子認證的信賴等級（LoA，Level of Assurance）[8] 概念，處理如何評估身分識別與電子認證的可信度及評定相關等級。每一個等級都有代表著對應的定義與評估標準，及所帶來的潛在衝擊。

1. LoA1 低度信賴等級：對宣稱或斷定的個體只有少許的信心或幾乎沒有信心。
2. LoA2 中度信賴等級：對宣稱或斷定的個體有某種程度上的信心。
3. LoA3 高度信賴等級：對宣稱或斷定的個體有高度的信心。
4. LoA4 最高信賴等級：對宣稱或斷定的個體有非常高度的信心。

NIST 800-63-3 進一步區分為三個流程：身分證明、驗證和聯邦式身分管理，並優化與調整原有LoA 2~3 定義不全的疑慮，整合為一套 XAL 標準。



圖六 LoA 對應到 XAL（NIST 800-63-3）規範（重製）

IAL 身分證明信賴等級：確定個人身份的身份證明過程的嚴謹性；選擇 IAL 是為了減輕潛在的身份證明錯誤。

- IAL1 – 在此等級，（若有提供）屬性是自我聲明的，或應該被視為自我聲明；沒有驗證過程。

[6] Paul A. Grassi, Michael E. Garcia, James L. Fenton (2017/06), Digital Identity Guidelines，來源：https://doi.org/10.6028/NIST.SP.800-63-3
[7] ISO/IEC 29115:2013 https://www.iso.org/obp/ui/#iso:std:iso-iec:29115:ed-1:v1:en
[8] 連子清，杜宏毅（2022）身分識別之書: 身分識別機制運作之原理原則

- IAL2 – 除須符合 IAL1 外，引入了遠端或親自身份證明的需求。至少需要使用SP 800-63A 中提供的程序進行遠端或親自身份驗證。
- IAL3 – 除須符合 IAL2 外，需要親自身分證明，如面對面或受監督的遠端身份驗證。必須通過檢查物理文件來驗證識別屬性，如 SP 800-63A 所述。

AAL 驗證信賴等級：確認驗證過程的嚴謹性，以及驗證器（Authenticator）與特定個人識別符之間的綁定。選擇 AAL 是為了減輕潛在的驗證錯誤（例如非法申請者使用不屬於他們的憑證）。

- AAL1 – 在此等級提供了一些保證，確保申請人控制著已註冊給使用者的驗證器。AAL1 要求使用各種可用的驗證技術進行單因素驗證。成功的驗證需要申請人通過安全的驗證協議證明對驗證器的擁有和控制。
- AAL2 – 提供高度確信，申請人控制著已註冊給使用者的驗證器。為了在 AAL2 進行驗證，申請人必須通過安全的驗證協議證明擁有和控制兩個不同的驗證要素。需要使用經批准的加密技術。
- AAL3 – 提供非常高的信心，確保申請人控制著已註冊給使用者的驗證器。在 AAL3 的認證是基於通過加密協議證明擁有密鑰。AAL3 與 AAL2 相似，但還需要一個提供驗證者冒充抵抗能力的加密驗證器。

FAL 聯邦式信賴等級：規範使用聯邦式斷言協議的嚴謹性。FAL 是非強制性的，因為不是所有數位身分系統都會利用聯邦式身份架構。選擇 FAL 是為了減輕潛在的聯邦式身份相關錯誤。

- FAL1：允許信賴方從身份提供者接收一個持有者斷言。身份提供者必須使用經過批准的加密方式對斷言進行簽署。
- FAL2：新增要求斷言必須使用經批准的加密技術進行加密，以便信賴方是唯一能夠解密的一方。
- FAL3：要求使用者提供與斷言中所述的加密金鑰參考及斷言本身的擁有證明。斷言必須使用經批准的加密方式簽署，並使用經批准的加密方式對依賴方進行加密。

3. 與 eIDAS 2.0 規範相關的數位身分驗證標準參考[9]

表二 數位身分驗證相關標準參考(重製)

	eMRTD (ISO 7501 – ICAO 9303)	eIDAS Token (TR-03110-2)	mDL (ISO/IEC 18013-5)	mID (ISO/IEC 23220)	X509 PKI certificates (ISO/IEC 9594-8)	SAML eIDAS (ITU-T	**OpenID Connect**	**OpenID Connect with SIOP**	**FIDO2** (ITU-T X.1278)	**SSI**
正式標準	O 國際	O 歐盟	O 國際	規劃中	O	O	X	X	O	X
個人身分識別資料 (PID) 格式	LDS1 eMTRD	LDS2 eMRTD/ Specific ASN.1 definition	mdoc mDL CBOR/ mdoc mDL signed JWT	mdoc CBOR, mdoc signed JWT (planned support for VC)	X.509 ASN.1 definitions	SAML assertion in XML format, according to an XSD definition	ID Token signed JWT	ID Token signed JWT (planned support for VC)	N/A	VC according to JWT, JSON-LD Anoncreds …
(合格)電子屬性證明格式	N/A	LDS2 eMRTD/ Specific ASN.1 definition	N/A	mdoc CBOR, mdoc signed JWT (planned support for VC)	X.509 and X520 ASN.1 definitions	SAML assertion in XML format, according to an XSD definition	ID Token signed JWT	ID Token signed JWT (planned support for VC)	N/A	VC according to JWT, JSON-LD , Anoncreds …
主體的離線認證	O	O	O	O	X	X	X	X	O	X
主體的線上認證 (LoA)	X	O	O	O	O	O	O	O	O	O
依賴方的離線認證	O	O	O	O	X	X	X	X	X	X
依賴方的線上認證	X	O	O	O	O	O	O	O	O	O
裝置綁定(例如智慧型手機)	X	選擇性	X	選擇性	選擇性	N/A	N/A	N/A	O	選擇性
使用安全元件(信賴程度)	X	O	X	X	選擇性	N/A	N/A	N/A	選擇性	選擇性
使用者單獨控制	X	O	X	O	選擇性	X	X	X	O	O
最初為執法機關設計	O	X	O	X	X	X	X	X	X	X
需要集中式身份提供者	X	O 需額外	O 只有伺服器相容	O 只有伺服器相容	X	O	O	O	N/A	X
選擇性披露	X	O	O	O	X	O	O	O	O	O
不可追蹤性/不可連結性	X	O	X	X	X	X	X	X	O	O

[9] ENISA (2023/07), DIGITAL IDENTITY STANDARDS, 來源: https://www.enisa.europa.eu/publications/digital-identity-standards

支援身份管理生命週期	發行/驗證/撤銷	發行/驗證/屬性共享/撤銷	發行/驗證/屬性共享/撤銷	發行/驗證/屬性共享/撤銷	發行/吊銷/撤銷/更新	驗證/屬性共享	驗證/屬性共享	驗證/屬性共享	驗證	發行/驗證/吊銷/撤回/更新
信任模型	聯邦式	聯邦式	聯邦式	聯邦式	企業/聯邦	企業/聯邦	企業/聯邦	聯邦式/去中心	中心化，可去中心但視驗證器決定	去中心化
標準的成熟度	高	高	中	低	高	高	高	中/低	高	中/低