

出國報告（出國類別：出席會議）

數位部參加美國第 38 屆網路身分工
作坊（**2024 Internet Identity
Workshop XXXVIII**）出國報告

服務機關：數位發展部

姓名職稱：李岳寅科長

黃彥霖資安制度工程師

派赴國家：美國

出國期間：**113.04.14-113.04.20**

報告日期：**113.04.25**

摘要

數位部本年（113 年）起執行數位創新基礎建設計畫之分散式驗證與授權系統（數位皮夾），即將採用具有數位身分自主權（Self-Sovereign Identity, SSI）相關國際標準，包含分散式身分（Decentralised Identity, DID）、可驗證憑證（Verifiable Credential, VC）與選擇性揭露（Selective Disclosure, SD）……等（詳細內容請參見官網公告之數位皮夾規劃草案¹）等，並確保全球互通的數位憑證能夠實踐，達成攜碼之實效。

網路身分工作坊（Internet Identity Workshop，以下簡稱 IIW）是全球分散式身分生態系的重要國際會議，一年舉辦兩次，已舉辦將近 20 年。過去重要成果包含與會者所制定的文件已成為全球資訊網協會（World Wide Web Consortium, W3C）的分散式識別符和可驗證憑證標準的規劃來源，更多的標準文件與相關草案也正在該場合制定中，實為分散式身分與網路身分的重要工作場合。該活動以開放空間會議（Open Space Technology, OST）形式進行，本次於民國 113 年 4 月 16 日至 18 日在美國舊金山舉辦，主題涵蓋數位身分自主權、分散式識別符、可驗證憑證、身分認證相關協議與多重因素認證等議題。與會者包括數位皮夾生態系多方關係人，如研究者、政策制定者、標準撰寫者、相關專家等。

本次會議也與各標準制定者或各國政府數位皮夾政策制定者進行深入交流，如美國加州行動駕照（Mobile Driver License, mDL）已經公開試點計劃，並使用上述討論之技術，本次出訪與加州數位轉型首席官交流其推行經驗，另本次會議也安排與開放皮夾基金會（Open Wallet Foundation, OWF）團隊成員交流分散式身分與可驗證憑證的公共程式與開放原始碼推行經驗。本次會議目標為積極推展符合國際發展的數位皮夾服務，強化導入國際網路標準，擴大臺美合作機會。

¹ <https://www-api.moda.gov.tw/File/Get/moda/zh-tw/u7filKS55Frifeo>

目錄

壹、	參與目的	1
貳、	參與行程	2
參、	參與概要	3
一、	拜會加州首席數位轉型官	3
二、	拜會開放皮夾基金會	9
三、	參與第 38 屆網路身分工作坊第一日	11
四、	參與第 38 屆網路身分工作坊第二日	17
五、	參與第 38 屆網路身分工作坊第三日	29
肆、	心得與建議	35
伍、	附錄	

壹、參與目的

網路身分工作坊為研議全球分散式數位身分生態系之重要國際會議，會議成果已成為全球資訊網協會之分散式識別符（DID）與可驗證憑證資料模型（Verifiable Credentials Data Model, VCDM）標準之規劃來源，此兩項標準亦納為本部本年數位創新基礎建設計畫之分散式驗證與授權系統（以下簡稱數位皮夾）規範依據。該會議每年舉辦兩次，以開放空間會議形式舉辦，本次定於113年4月16日至18日在山景城舉行，此次大會議題將圍繞身分自主權、分散式識別符、可驗證憑證、身分認證相關協議（如：OpenID Connect、FIDO2等）、多重因素認證（MFA, multi-factor authentication）、身分與物聯網等。此次與會者包含數位皮夾生態系研究者、政策制定者、各標準撰寫者、開源專案相關工程師等。本次出訪於工作坊分享本部數位皮夾規劃草案並和與會成員交換意見，並討論潛在合作之可行性；另外，美國加利福尼亞州車輛管理局（California Department of Motor Vehicles, CA DMV）已運用憑證技術核發行動駕照，經本司接洽對方同意由加州首席數位轉型官（Chief Digital Transformation Officer）阿賈伊·古普塔（Ajay Gupta）於4月15日與我國分享交流其行動駕照推行經驗，併同參訪該局交流臺美數位憑證運用經驗。此行同時安排與開放皮夾基金會（OWF）團隊成員交流分散式身分與可驗證憑證之公共程式與開放原始碼推行經驗。

本次出國規劃目的明確，為在數位皮夾規劃執行階段便積極推展有利於我國發展符合國際標準趨勢之數位服務，並強化導入國際網路標準及擴大臺美合作機會。詳細內容分述於參與行程內文。

貳、參與行程：

本次參與第 38 屆網路身分工作坊行程自 113 年 4 月 14 日至 113 年 4 月 20

日合計 7 日，行程安排如下表：

表 1 參與美國第 38 屆網路身分工作坊行程表

日期	活動內容
113.04.14(日)	● 啟程前往美國加利福尼亞州
113.04.15(一)	● 拜會加州首席數位轉型官 Ajay Gupta ● 拜會開放皮夾基金會
113.04.16(二)	● 參與第 38 屆網路身分工作坊
113.04.17(三)	● 參與第 38 屆網路身分工作坊並發表臺灣數位皮夾規劃草案
113.04.18(四)	● 參與第 38 屆網路身分工作坊
113.04.19(五)	● 啟程返回臺灣
113.04.20(六)	● 返抵臺灣

參、參與概要：

本次行程涵蓋有關分散式身分、數位憑證等議題之多方關係人，涵納產官學社各方代表，官方部分包含加州州政府數位轉型部門與車輛管理局、德國破壞創新聯邦總署（Federal Agency for Disruptive Innovation, SPRIND）、加拿大卑詩省（British Columbia）數位皮夾開發者、不丹數位皮夾開發者等；產業面包含數位皮夾技術提供者、開發者、大型跨境平台、作業系統與瀏覽器開發商，這些參與者在數位皮夾生態系皆扮演重要角色；社群面包含分散式識別符、可驗證憑證、選擇性揭露、行動駕照標準（如國際標準組織所制定之 ISO 18013 規格）等互通規格的國際標準制定組織（Standards Development Organization, SDO）成員。此外本行一大目的也包含數位皮夾如何走向開放原始碼，乃至於符合全球公共程式（Public Code）走向的我國政策方針。因此本次行程除參考各國政策制定者如何推行數位皮夾與相關憑證外，也對我國遵循相關國際標準發展具有顯著效益。

一、拜會加州首席數位轉型官

美國加利福尼亞州於 112 年底推出名為「行動駕照」（mDL）的數位身分證明試點計畫，是美國官方進行數位身分皮夾（Digital Identity Wallet）的指標性先期亮點計畫，本次於 4 月 15 日前往加州首府沙加緬度（Sacramento）的加州車輛管理局總部拜會加州數位轉型首席官 Ajay Gupta 就數位皮夾計畫交換部署與應用意見，並就國際合作可行性進行初步討論。



圖 1、與加州數位轉型首席官 Ajay Gupta 合影

美國並無統一身分證，再加上美國國人使用汽車人口比例大，因此在紙本時代，駕照便為識別美國公民身分的重要證件。在數位轉型的過程中，「行動駕照」便是重要的數位憑證。根據 Ajay 表示，加州人口目前為 3,900 萬左右，領有加州駕照的人數約有 3,100 萬人，覆蓋率廣，因此加州「行動駕照皮夾」（CA DMV Wallet）便是以此為基礎進行數位轉型。目前美國各州針對身分憑證放入皮夾的做法有諸多不同嘗試，比如與行動作業系統供應商直接合作，將行動駕照放入作業系統之預設皮夾中，如 Android 系統的 Google Wallet 與 iOS 系統的 Apple Wallet 等；也有如加州開發自己的應用程式皮夾，與供應商合作，推出自己的服務。目前，亞利桑那州、科羅拉多州、喬治亞州和馬里蘭州支援在 iPhone 和 Apple Wallet 上使用數位駕照，

而只有馬里蘭州的數位身分證可以在 **Android** 和 **Google Wallet** 上使用。此外，夏威夷、路易斯安那州、密西西比州、俄亥俄州和猶他州也有應用其他服務的數位卡片。

目前美國聯邦政府國土安全部已推出數位身分服務 **Real ID** 十年有餘，其覆蓋率並沒有如駕照這麼廣，根據 **Ajay** 表示，加州行動駕照皮夾的使用者可以選擇相容於 **Real ID** 服務，也可以選擇僅符合加州駕照資格。此外由於國土安全部相關規定，美國使用之數位憑證以國際標準組織所發行之 **ISO 18013 (mobile driver licence, mDL)** 為主，但是加州之行動駕照目前也兼容由網路資訊協會 (**W3C**) 所頒布之可驗證憑證 (**Verifiable Credential, VC**) 標準，為目前美國唯一採用相關標準之政府組織憑證。且該皮夾服務正在往「三合一憑證整合」為目標，分別為行動駕照、車輛登記號碼相關憑證與車輛保險證明，橫跨駕駛行為所需的所有憑證，除了行動駕照被聯邦政府特別規範之外，其他憑證正在以可驗證憑證作為開發方向。此外值得期待的是，加州行動駕照即將開放原始碼，成為美國公共程式 (**Public Code**) 的指標案例之一。

加州行動駕照仍在試點階段，從 **112** 年底開始直到 **115** 年，已服務 **30** 餘萬公民，目標試點最大容量為 **150** 萬人，這個階段的目標是「管理數位憑證生命周期的能力，例如行動駕照、軟體審計與專業認證等。」目前主要的應用為必須進行年齡確認的零售服務（如煙草、酒精等）、國內機場通關服務、身分確認等，這部分使用美國運輸安全管理局 (**Transportation Security Administration, TSA**) 所核可之驗證機器，讓行動駕照能完成自動化驗證的服務流程，目前已可在美國國內機場關口見到相關機器。值得注

意的是，該行動駕照以 ISO 18013 為相容標準²。

除此之外，加州行動駕照有一個特色為其使用的開放原始碼套件 SpruceKIT，兼容於 W3C 可驗證憑證標準與 ISO 18013 行動駕照標準，從而實踐可互通性，這有助於在跨境、跨平台與跨服務層次彼此互相溝通必要資訊，免於平台壟斷（Vendor Lock-in）的風險。這兩種標準各有好處，Ajay 認為 W3C 可驗證憑證標準較適合遠端認證如線上認證等，而 ISO 行動駕照標準比較適合近端通訊如藍芽等。在兼容標準的工作進程上，加州行動駕照皮夾採用了 OpenID Foundation 的 OpenID4VCI 與 OpenID4VP 標準作為介接。在標準相容性上，我們討論了可驗證憑證的標準藍圖目前仍然未定之天，有許多標準還尚待整合，如網際網路工程任務組（Internet Engineering Task Force, IETF）所開發之 SD-JWT（Selective Disclosure JSON-Web Token）或是關聯資料（Linked Data）相容之可驗證憑證等等，目前還有待觀察。

在會議上我們都對於有關身分憑證的不同標準之設計目的具有共識，ISO 18013 的發展脈絡是以政府服務為核心的權威機關（Certificate Authority）為目標對象進行標準制定，如車輛管理局（DMV）等監理機關，或是其他政府相關之發證機構如臺灣之健保署、內政部等，都算是服務範圍。其設計原理又與過去的複雜的數位身分標準 ISO/IEC 29115（資訊科技法人認證與確認框架）不同，簡化了繁複的憑證發行與依賴方（Relying Party, RP）關係。自 ISO 18013 之後，由於駕照之數位化設計有不少先天限制，後續衍生出尚未成熟之新興標準 ISO 23220，將行動駕照（mDL）修改成適用範圍更廣之行動文件（mobile document, mDOC）。基於權威機構的主導性，該

² <https://blog.spruceid.com/spruceid-partners-with-ca-dmv-on-mdl/>

標準具有集中化管理，便於管制的特色。值得注意的是在隱私保護的精神上與可驗證憑證（VC）有所差異，前者為資料最小化（data minimization），後者為選擇性揭露（Selective Disclosure, SD），可以看出主從性的不同，前者講求主導機構從源頭降低資料外洩的可能性，後者講求使用者自主與知情同意的精神。而可驗證憑證與其相關連之分散式識別符標準（DID），便是基於數位身分自主權（SSI）為精神進行規劃，以分散式兼容為基底，優勢在於其相關憑證不需透過中央權威機構進行承認，便於多方關係人之憑證生態系發展，缺點在於不同組織採用之解決方案不統一，生態系各層次的服務商需要花費更多精力來相容不同機構之服務，這也是本次網路身分工作坊的熱門討論主題之一。

回到車輛管理局行動創新業務，根據 Ajay 表示，加州車輛管理局正在以 CA DMV Wallet 皮夾服務為基底，持續開發出許多加值服務，如「以行動駕照登入」（Sign-in with mDL）服務，讓數位皮夾也具有「單一登入」（Single Sign-on, SSO）之功能。我們也討論到行動駕照未來是否也有「電子簽章」（electronic signature）之功能，Ajay 表示目前行動駕照的簽署功能以相關服務之電子文件保護為主，如以行動駕照之公私鑰對（Public-Private Key Pair，為經由非對稱加密演算法產生之獨一無二之簽署工具）進行殘障車位文件（Disability Certificate）進行加密保障，並且可以轉移到不同行動載具，方便使用者可以跨裝置使用電子文件。這是因為殘障人士並不一定只會搭乘單一車輛，在數位世界中，一方面讓電子文件具有資料可攜性，另一方面也具有資料真實性（Data Integrity），完成虛實整合之效果。

另外我們也針對行動駕照的「範圍外使用」進行討論，在臺灣許多憑證都有嚴格規範使用範圍，如健保卡只能使用於全民健康保險資料登入等作業，但實際上健保卡也能作為雙證件使用，在數位轉型的過程中，相關

需求日益增加，既有規定可能難以規範驗證者之使用範圍，因此以此作為題目與 Ajay 討論。Ajay 認為基於駕照本來在美國就作為重要身分證件，其實許多場景都是以駕照之屬性欄位（attribute）進行驗證，如年齡驗證（Age Verification）便為接下來試點計劃的重要驗證場景，而目前加州行動駕照也以電商平台作為試點案例，特別是菸草、酒精飲料的線上銷售服務。當然在某些特許情境下，如領證執照驗證（餐廳執照、衛生稽查員執照等）本來就不應該使用行動駕照進行驗證。因此建議應以屬性資料是否滿足驗證場景需求作為評判標準。

最後我們也討論加密錢包（web3 wallet）與數位身分皮夾（digital identity wallet）是否能夠整合進行初步討論。事實上加州車輛管理局相關憑證早期以 Tezos 區塊鏈進行驗證³，Tezos 是世界上早期的權益證明（Proof of Stake）開放區塊鏈，不會因為算力需求而耗費電力，具有綠能環保等特色。加州行動駕照如同本部發展方向，先有以區塊鏈作為基底的憑證互通性測試，後來確認民眾具有行動裝置皮夾服務的需求之後，以開發符合「公共程式」精神的皮夾服務做為目標，這是因為對於身分憑證而言，持有者（holder）仍然缺乏成熟的基礎建設，對於大眾使用者而言，能夠從手機作業系統下載安裝的應用程式才是比較習慣使用的服務（意為 web2 服務，web3 服務的 Wallet App 多數以網頁應用程式或瀏覽器外掛程式為主）。不過 Ajay 表示，加州行動駕照仍然在探索與 web3 服務整合的可能性，加州行動駕照正在規劃發行以非同質化代幣（Non-fungible Token, NFT）整合可驗證憑證（VC）形式的數位憑證，讓憑證得以擁有更彈性的應用場景，如抗共謀攻擊（Anti-collision attack）與真人證明（Proof of Personhood）等，這些憑證不會用在「駕照」，但會用在更多多元的應用場景，如車輛

³ <https://cointelegraph.com/news/california-dmv-to-digitize-car-title-management-system-via-tezos>

憑證、保險憑證或更多物權、資格證明等等。我們也將本部於 112 年進行的驗證專案 TW-DID 分享進行交流，TW-DID 以可驗證憑證形式將行動自然人憑證（TwFiDO）發放至申請者之以太坊地址（Ethereum Address），讓使用者未來有身分證明需求時可以使用該可驗證憑證。此過程使用零知識證明（Zero Knowledge Proof）為加密方法，讓外部無法破解申請者之真實身分，除非使用者知情同意願意自我揭露。在這段討論中，我們與 Ajay 都同意目前數位身分皮夾與 web3 錢包相容的問題是，對於公共服務（Public Service）而言，究竟需要滿足多廣泛的 web3 需求還是一個需要深究的主題。如不同區塊鏈有不同的智慧合約（Smart Contract）撰寫形式，更不用說除了公共區塊鏈之外，還有聯盟鏈（Consortium Blockchain）作為某些地區的公共服務。我們認為開放生態系並且有限度的開放皮夾憑證的介接標準，可能可以促進相關服務成熟，尤其是在生態系仍在建構的初期，有需求便會有相關的服務商誕生。

最後，電子前哨基金會（Electric Frontier Foundation, EFF）於 113 年 3 月在查看加州行動駕照資訊後提出了幾點建議⁴，包含重視選擇性揭露功能、將開放皮夾原始碼並創造互通可能性、建立公眾溝通管道、並促進使用者設計讓使用者能自主掌握皮夾功能。也撰文倡議關注公民數位隱私，尤其是當數位皮夾作為行動裝置應用程式時所引起的相關風險，該文並呼籲州政府及其供應商更加關注使用者的保護，其細節可參考《解讀加州行動駕照》（Decoding the California DMV's Mobile Driver's License）⁵

⁴ Decoding the California DMV's Mobile Driver's License, <https://www.eff.org/deeplinks/2024/03/decoding-california-dmvs-mobile-drivers-license>

⁵ <https://www.eff.org/deeplinks/2024/03/decoding-california-dmvs-mobile-drivers-license>

二、拜會開放皮夾基金會

此行也包含拜會「開放皮夾基金會」(Open Wallet Foundation, OWF) 執行長 Daniel Goldschneider 與其同僚。OWF 是 Linux Foundation 旗下的開放倡議組織，總部位於比利時布魯塞爾，目前成立一年有餘。OWF 由開放原始碼社群的技術開發者為主組成，共同合作開發基於開放標準的開放原始碼程式皮夾套件，由發行者、皮夾提供商和驗證者可以使用皮夾組件來實踐，以保護使用者的安全和隱私。Linux 基金會於 104 年營運開發以區塊鏈協議為主的組織，名為「超級帳本」(Hyperledger)，處理不同領域資料記錄與互通的解決方案，包含金融聯盟鏈、數位身分解決方案等等。而 Linux 基金會有感於數位身分與數位皮夾不僅止於區塊鏈領域，因此於 112 年成立開放皮夾基金會，以開放原始碼精神創立可互通的數位皮夾專案，其探討主題包含數位身分皮夾與金融電子錢包服務，並且另設「政府諮詢委員會」(Government Advisory Council, GAC) 縫合政府與民間意見與需求。「政府諮詢委員會」是 OWF 旗下委員會，代表政府和政府間組織在 OWF 中的意見，促進多方利益相關者合作，參與國家目前有阿根廷、不丹、愛爾蘭、義大利、中國、墨西哥、巴布亞新幾內亞、葡萄牙、瑞典、瑞士、英國和美國。其成員包含現任主席為英國卡羅爾·巴特爾 (Carol Buttle)，Carol 是英國科學、創新和技術部 (DSIT) 的認證、保證和安全 (CISO) 主管。她在反恐、軍事、國防、政府和醫療等領域擁有數十年的經驗，開發了數位身分解決方案、皮夾和英國政府的信任框架；美方代表為美國國家標準暨技術研究院 (NIST) 之身分計畫主席 (Identity Program Lead) 的 Ryan Galluzzo 等。GAC 政府代表資格必須是由主權國家政府 (聯合國會員國) 任命的代表，其主要職能包括在電信、資訊和通信技術 (ICT)、網路

安全、數位經濟和社會、**數位進程**、科技創新、網路政策等領域制定或影響政府或公共政策。另外 OWF 協作組織參與，包含 GAC 皆無需額外支付費用。GAC 政府代表功能為可能影響數位皮夾事務的公共政策問題，向 OWF 執行委員會提供建議，包括：確定並提供建議有關公共政策問題，特別是在 OWF 的活動與國家法律或國際協議之間存在互動的狀況下。此外 OWF 也有兩個團隊分別開發皮夾服務，分別為荷蘭團隊 Credo 與來自加拿大的 Bifold 團隊，Bifold 團隊又成為卑詩省官方皮夾的基礎技術（詳見後續章節說明）。對於 OWF 而言，開放皮夾的意義在於使數位憑證、數位憑證容器（皮夾）與硬體裝置可以解耦，使不同功能的皮夾可以多元共生，讓使用者不會被超級應用程式（SuperApp）所綁定，或遭致供應商壟斷（Vendor Lock-in）之情形。這與本部「數位皮夾」相關設計原則相仿（相關簡報見附錄 2⁶）。

我們於會議中與 OWF 相關成員交換意見，討論以臺灣為目標的數位皮夾生態系應如何發展，並介紹臺灣「公共程式」（Public Code）精神與相關專案，規劃數位皮夾相關套件接下來以開放原始碼之公共程式發表，並促進國內與跨境應用案例。該組織也介紹了德國與加拿大執行數位皮夾專案的成員與我們交流，進一步討論潛在技術合作的可能性。

⁶ 附錄 2、2024-OpenWallet-Presentation

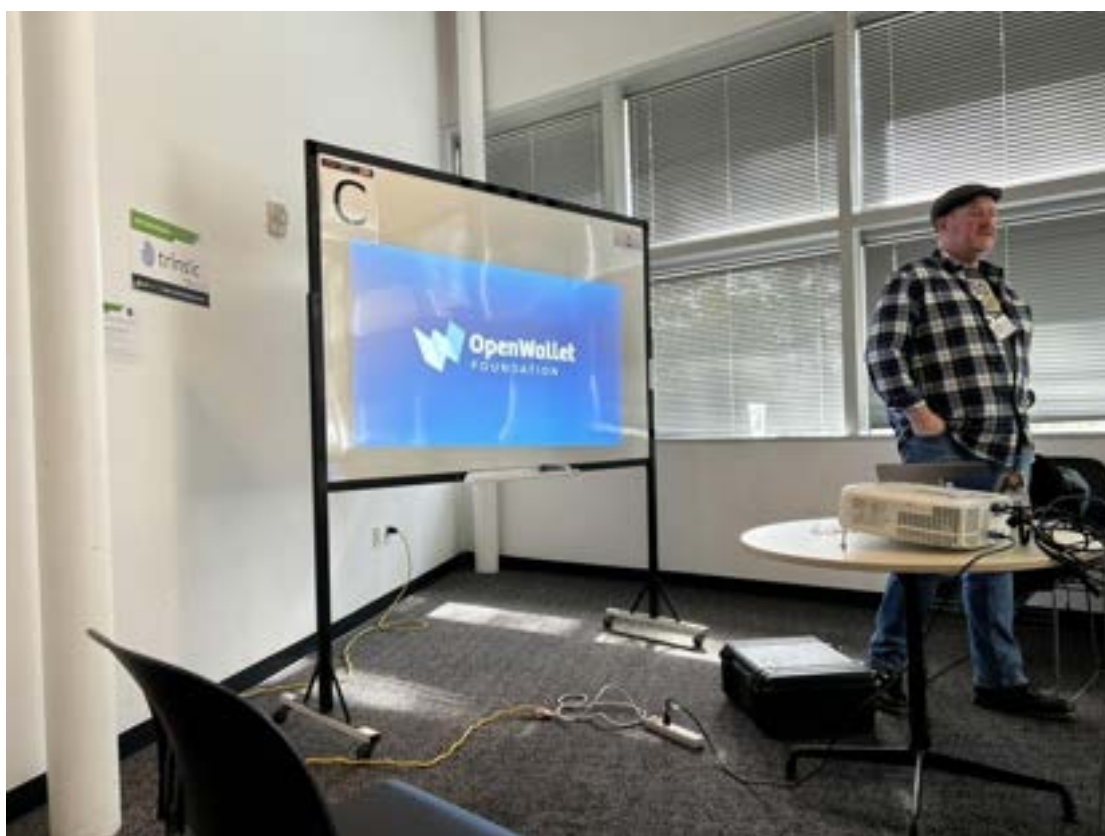


圖 2、拜會開放皮夾基金會

三、參與第 38 屆網路身分工作坊第一日

第 38 屆網路身分工作坊中在加利福尼亞州矽谷山景城（Mountain View City）的電腦史博物館（Computer History Museum）展開，參與者三百多人，來自世界各地，為有關網路身分的多方關係人，以跨境平台、新創機構與標準開發組織（Standards Development Organizations, SDOs）開發者為主流。為期三天的活動多以「非會議」（unconference）為形式舉辦，每日第一個活動環節，所有人都可以提案寫下自己想要討論的主題，許多組織早已準備好分享内容，如開放身分基金會（OpenID Foundation）的成員在第一日分享 OpenID Connect、OpenID4VC 等標準進度、網際網路工程任務組（Internet Engineering Task Force, IETF）成員分享選擇性揭露

JSON 網路權杖憑證 (SD-JWT VC) 開發進度，有些皮夾 (Wallet) 開發者也會分享自己的服務開發進度等。



圖 3、大會以「非會議」形式進行，圖中各色紙為第一日議程內容

網路身分工作坊相關主題範圍廣泛，第一場為分散身分基金會 (Decentralised Identity Foundation, DIF) 成員分析網路身分演變脈絡，分散式身分概念便是自 104 年開始從本工作坊發展而來，即使數年來許多大型跨境平台服務如 Google、微軟多作為贊助者參與此活動，本身也會派員參與標準制定與專案開發，取得標準制定的先機，因此網路身分工作坊仍具有濃厚的開放原始碼、點對點 (peer-to-peer) 通訊精神，與網路初期建置風格相近。根據 DIF 成員介紹，104 年自公共區塊鏈以太坊 (Ethereum) 發表啟動以來，英美政府與相關標準社群對於區塊鏈身分 (Blockchain Identity) 如何可以成為公共服務或協助數位轉型過程產生興趣，這是因為區塊鏈作為一種分散式帳本技術 (Decentralised Ledger Technology, DLT)，使用無許可 (permissionless) 的帳本公開紀錄，具有防竄改 (Tamper-

Proof) 特色，因此在許多應用情境下，其服務是具有產業價值的。在後續九年間，分散式身分乃至於數位身分自主權 (SSI) 等概念開始被提出，直到 111 年相關技術被全球資訊網協會 (World Wide Web Consortium, W3C) 以分散式識別符與可驗證憑證資料模型 (第 1.1 版本) 標準化，後續相關標準進入百花齊放的時代，在此次工作坊中，可以看到不同組織以「草稿」形式發表意見，甚至也有出現標準格式衝突並且進入辯論的情形。其實光是 W3C 本身除了可驗證憑證工作組及分散式身分工作組以外，還有網路孵化器社群組 (Web Incubator Community Group, WICG) 針對數位憑證應用程式介面 (Web Credential API) 進行開發討論，彼此之間呈現競合狀態。

統整網路身分工作坊討論議題，以概念性光譜而言可以分為**數位身分自主權 (SSI)**、**分散式身分**、**數位憑證**與**數位皮夾**四項。此四項互有交集，概念上卻有所不同 (如表 1)。

表 1、新興網路身分概念盤點

多元並立的自主體系概念		網路信任層的交換體系工具	
分散式身分	數位身分自主權	數位憑證	數位皮夾

首先政策制定者比較喜歡使用數位身分自主的概念，而非分散式身分，這是因為從各國政府視角而言，政府證件與政府憑證數位轉型的過程中，很容易陷入中心化管制與數位足跡追蹤的輿論壓力中，因此如何在公共服務的規劃設計上，讓公民可以自主管理自己的個人資料，就是首要考量；而分散式身分在標準定義上是一種識別符 (Identifier)，如同 HTTPS 網址或其他位址服務，是身分作為一種網路層的交換形式，但是在這幾年區塊鏈技術快速發展的進程上，分散式身分也被用作與「集中式身分」

(Centralised Identity) 的對立形式，在服務提供者與使用者的敘事上，分散式身分具有自外於權威發證機構 (Identity Provider, IdP) 或依賴方 (Relying Party, RP) 的設計形式，因此這也是為何政策制定者多數習於使用 SSI 而非 DID 的原因，畢竟政府本來就是各司法管轄區 (Jurisdiction) 最大的發證機構，再怎麼設計也很難避免特許、集中式信任關係，最佳設計方式便是積極使政府在技術上與法規上避免侵害數位公民隱私、個人資料等議題。而數位憑證與數位皮夾又與前兩者有所互補，數位憑證並不一定是分散式的，根憑證 (Root Certificate) 或信任鏈 (Chain of Trust) 等概念早已用於日常網路活動，但是自新一代「可驗證憑證」(VC) 標準被制定且實作以後，許多憑證服務更加分散式化，使用者與驗證者可以不再依賴傳統憑證的權威機構，一方面提升了網路認證服務的自由度，另一方面下降了集中式組織的控制力。在數位憑證領域，其認證方法不只限於網路位址與可信內容，也慢慢產生了更多樣化的服務，如個人身分憑證 (如真人證明、國家級身分資格、特許執照等)、個人資料憑證 (學歷或考試證明、相關福利資格、健康資料或特定服務衍生資料憑證) 或非人的機器憑證 (如電動車等物聯網所需憑證、貨物交易憑證等)、有價資產憑證 (如金融憑證、碳權憑證等等)。以上概念若需要在數位化世界有效交流，便需要數位憑證作為成熟技術，且需要被牽涉其中的多方關係人 (multi-stakeholder) 所承認，因此無論是學術組織、政府組織還是國際組織，皆提出網路的互聯模型 (Interconnection Model) 中，其分層應該要有「身分層」(Identity Layer) 的呼籲，如日本提出信任網路 (Trusted Web)、web3 領域也出現靈魂綁定代幣 (Soul Bound Token, SBT) 或社會圖譜人格證明 (Social-Graphed Based Proof of Personhood) 等。關於數位憑證的新興技術，目前有許多標準與服務正在建構中，其核心概念包括選擇性揭露

(SD)、資料最小化、資料可攜性等等，目前正在技術成熟的階段。而數位皮夾 (Digital Identity Wallet, DIW) 則為較新穎的概念，當數位憑證成為一個必然出現的網路服務後，憑證便需要容器作為交換與驗證的位址，因此基於分散式身分的皮夾服務應運而生。數位皮夾在不同的關係人結構中運作的樣貌截然不同，比如目前行動作業系統服務商所提供的皮夾服務多為相容其電子支付、數位支付服務，如 Apple Wallet、Google Wallet、Samsung Wallet 等，其積極與各地政府合作，試圖將各地公民身分憑證納入其皮夾生態系中，因此多使用上一章所描述之行動駕照 (mDL) 標準；而對於第三方皮夾開發商而言，其容納之數位憑證不一定是集中式身分或透過權威機構所頒發的憑證，因此作為應用程式更適合接收與驗證更多元目的之數位憑證。此外也有些政府服務已開發獨立營運的皮夾服務，如不丹、加拿大卑詩省與美國加州等。此外除了智慧型手機的應用程式外，瀏覽器的皮夾服務也正在成熟中。綜上所述，皮夾生態系正處於先期階段，各地與各項服務所開發之數位憑證、數位皮夾、發行者與驗證者彼此之間是否可以互通，使用標準、數位格式如何兼容，便是網路身分工作坊的核心議題之一。舉例而言，由 IETF 所開發之 SD-JWT VC 與 W3C 所頒布之關聯資料 (Linked Data, LD) 之可驗證憑證資料模型 (VCDM) 便不容易互通，前者已被歐盟數位皮夾框架所適用，後者由於難度較高，開發進度趨緩，因此在會議中也有人提出 SD-JWT VCDM 模式，讓兩方有互通的可能性。

以下統整進階討論議題成果，分為「國際組織」、「分散式身分交互模解決方案式」、「政府專案案例」與「標準類別」等。在第一日國際組織介紹方面，計有分散式身分基金會 (DIF) 與 Linux 基金會旗下之開放皮夾基金會 (Open Wallet Foundation, OWF)，OWF 已於上文介紹便不贅述。DIF 為以開發者為主，是 Linux 基金會旗下組織，自外於 W3C 分散式身分工

作組成立之多方關係人組織，其核心精神以推廣分散式身分為主，旗下有許多工作組，最重要的服務便為整合不同分散式識別符方法（**DID Method**）的分散式身分通訊（**DID Coomunication, DIDComm**），讓百花齊放的分散式身分生態得以互通，此外還有憑證開發（**Presentation Exchange v2**）、安全資料儲存（**encrypted data vault**）、應用加密套件（適用於 IETF 的 **BBS+** 加密套件）、識別符的新增功能（如金鑰輪轉 [**Key Rotation**] 或金鑰撤銷 [**Revocation**] 等）、皮夾安全、分散式身分認證（如 **OIDC4VC** 與 **OIDC4VP** 標準，現已轉移至開放身分基金會工作組進行）...等。DIF 核心工作方向為創造組織性合作、技術文件建置、參考資料導入與產業合作等（見附錄 3⁷）。在交互模式解決方案方面，總共討論了 **DIDComm**、**OpenID for VC (OID4VC)** 標準草案、金鑰事件收據基礎建設（**Key Event Receipt Infrastructure, KERI**）、選擇性揭露 **JSON** 網頁權杖（**SD-JWT**）等（見附錄 4⁸）。

政府專案部分計有歐盟區塊鏈服務基礎建設（**European Block Chain Service Infrastructure, EBSI**），其服務框架正在因應歐盟數位身分、認證與信任框架（**eIDAS2.0**）通過而進行修正，目前也提供給組織、使用者可測試的皮夾環境進行憑證互認，並試圖從官方的區塊鏈架構重新設計信任鏈架構，如根可信任憑證組織（**Root Trusted Accreditation Organisation, rTAO**）等便是新興數位身分信任模式。此外也討論了美國聯邦政府國土安全部於 20 年前頒布的 **RealID** 與新型態的行動駕照之間的法規調適。另外有關歐盟各國因應數位皮夾已經法制化⁹，大規模試點案例正待執行，各地已啟動各自的補助或徵求專案，如德國數位皮夾創新補助專案由 **SPRIND** 組織執行，

⁷ 附錄 3、Intro to SSI and DIF- Spring 2024 IIW

⁸ 附錄 4、KERI-IIW38

⁹ eIDAS 2.0 – The European Digital Identity Framework Regulation heads to enactment

可供本部借鑑，詳述於後。

相關標準部分，參與場次主要為由國際標準組織（ISO）工作組成員分享行動駕照標準的後續擴充進度，即為行動文件標準（ISO 23220, mDoc），ISO 23220 以簡明二進制物件表示法物件簽署和加密（COSE）還有簡明二進制物件表示法基礎資料（CBOR-based Data）作為格式基底，並且解決了 ISO 18013-5 以近場通訊為主，並沒有線上認證相關規範的問題，進一步擴充了數位身分證應用的範圍，不過會中與會者也就 SD-JWT VC 與 ISO 23220 之間的異同與衝突進行討論。就目前業界而言，多數仍採用 ISO18013-5 相關規範，ISO 23220 屬於甫發布的新興標準，尚未有大規模採用的案例。



圖 4、ISO 小組參與者分享了電子文件（mDoc）使用的理據，主要方向為政府數位憑證服務的新一代準則。

四、參與第 38 屆網路身分工作坊第二日



圖 5、第二日議程

第二日分為兩個主要環節，分別為快速展示（Speed Demo）與非會議，我們在快速展示分享了數位部於 112 年進行的概念驗證專案 TW-DID 與 114 年即將啟動的數位皮夾（DID Wallet）規劃草案，相關簡報隨附於附錄 1¹⁰。非會議部分，今天主要議程集中在與網路身分相關組織與活動的盤點，相關多邊組織、多方關係組織與活動多達十數種，相關成員與主席皆有與會本次會議，這個機會為我們評估未來各式國際活動與潛在國際合作帶來具體成效；另外也有討論議程的目的為重新盤點網路身分的高階概念（high-level）原則。21 世紀以降，已有多個國際組織與網路運動倡議者針對網路身分設計原則提出論證，以確定在架構設計上，何種網路身分架構可以保護隱私安全與數位人權，相關文本參考了 112 年 10 月由開放身分基金會

¹⁰ 附錄 1、DID Wallet Draft Introduction 2024/04 IIW & CA DMV

(OpenID Foundation) 發表的《為政策制定者所寫的以人為本的數位身分》(Human-Centric Digital Identity: for Government Officials)，詳見後述。這些原則也衍生出近幾年來各組織所開發之國際標準；此外我們也探討了全球南方 (Global South，多為開發中國家) 如何使用共通套件打造聯邦式的數位身分 (Federated Digital Identity)，做為數位公共基礎建設 (Digital Public Infrastructure, DPI) 的一部份，以降低開發成本，該專案名為模組化開放原始碼身分平台 (Modular Open Source Identity Platform, MOSIP)，該專案衍生自印度集中式數位身分平台 Aadhaar，會中也針對各國政府所推出的數位身分架構進行討論，特別是數位足跡追蹤與紙本權利相關議題；會中也有「超越網際網路信任協定之信任架構」(Trust over IP, ToIP) 議題進行討論，可以說是網路基礎身分層建構與各式有關分散式身分與可驗證憑證工具應用的集大成者；最後議程也針對甫通過法制確認的「第二代歐盟身分、認證與信任架構」(eIDAS2.0) 與歐盟區塊鏈服務基礎建設 (EBSI) 之間如何創造信任鏈 (Chain of Trust) 進行討論與原型展示¹¹。

¹¹ <https://hub.ebsi.eu/conformance/build-solutions/accredit-and-authorise-functional-flows>



圖 6、於快速展示環節展示臺灣數位部之數位皮夾規劃，前排中為開放身分基金會執行長與電腦科學家崎村夏彥（Nat Sakimura）

「快速展示」（Speed Demo）為網路身分工作坊中提供各國政府、各開發團隊展示原型服務的場合，共計有 20 組團隊進行發表，其中政府服務提供者本次有 2 個團隊與會，分別為本部數位皮夾規劃與不丹國民皮夾（Bhutan NDI Wallet）服務。於本次展示中，我們介紹了民國 112 年的概念驗證專案 TD-DID，透過行動自然人憑證（TwFiDO or Digital Citizen Certificate）發放可驗證憑證與以太坊區塊鏈地址進行綁定，此間使用 did:web 方式進行實作，並且使用零知識證明（Zero Knowledge Proof）技術之套件 Semaphore 確保個人資料與臺灣人身分不會外洩，詳細敘述可參考該專案參與者朱昱任（Yuren Ju）所著文章《概念驗證：隱私優先的臺灣居民數位身分》¹²；再來我們分享了 113 年至 116 年的數位公共建設專案數位皮夾，簡介了臺灣數位身分的發展脈絡，並展示本部對於網路分散式、點對

¹² https://yurenju.blog/posts/2024-02-04_taiwan-digital-id-privacy-first/

點通訊本質的架構設計。本部將於 113 年實作並開放數位皮夾相關套件，以分散式身分與可驗證憑證為藍本，設計有關數位皮夾可互通性的協定，協助各部會、各發證服務針對既有憑證發行可驗證憑證作為互通，並釋出皮夾原型與其原始碼供民眾與技術專家審視。數位皮夾的未來方針為儘速使公民、相關產業與公共部門可以自行發行與驗證經過充分加密保護的可驗證憑證，並以生態系觀點發展相關網路基礎架構。

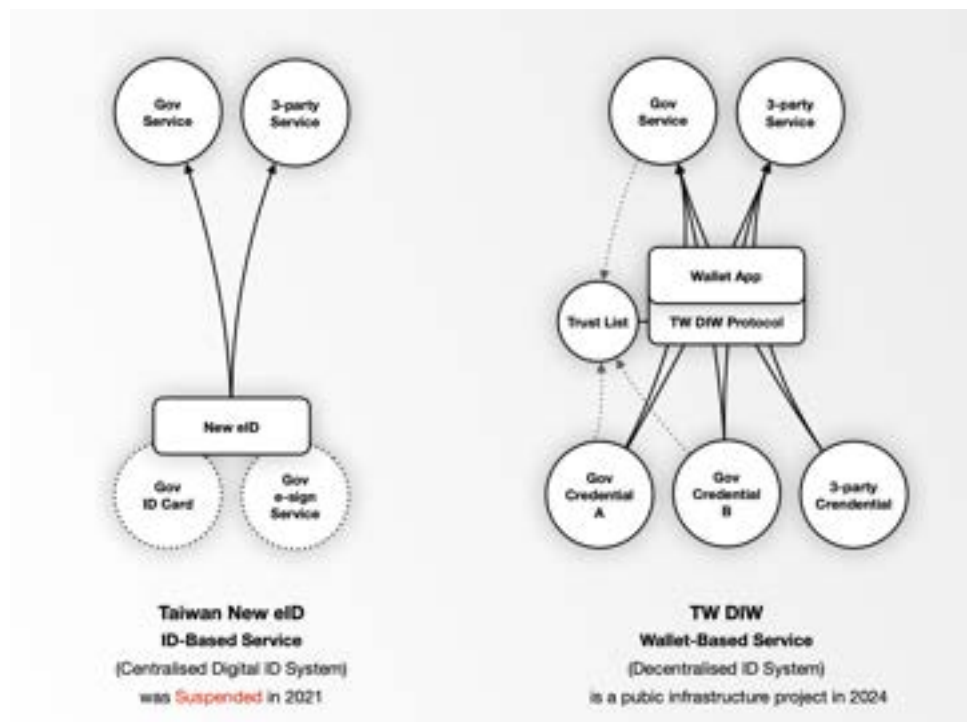


圖 7、簡述數位皮夾專案的分散式結構設計

數位皮夾的設計架構與概念獲得許多技術專家的讚賞，包含 did:web 的核心開發者。我們所規劃之開放、互通、韌性與降低權威機構的方向符合許多網路身分層、分散式身分標準制定者的理念。同時我們也分享了臺灣在數位領域願意積極進行國際合作的決心，以數位皮夾為藍本，其技術合作層次可以提升國內數位服務的全球互通性，並就網路身分層的未來產業生態系即早佈局。最後美國國土安全部（Department of Homeland Security, DHS）官員也對數位皮夾規劃產生興趣，未來具有潛在深入探討雙方技術

標準的可能性。



圖 8、於快速展示環節展示臺灣數位部之數位皮夾規劃，圖前排發言者為 Google Wallet 核心開發成員

非會議部分，首先討論有關網路身分相關組織與活動地景。本次討論聚焦於數位身分相關貢獻者與多方關係人的現況，包括各式組織、標準及會議活動。與會者在探討數位身分、網路身分或分散式身分運作時，先初步盤點了眾多非營利組織（NPOs）和標準制定機構（SDOs），並進一步討論它們之間的分歧。這個議程的共識是與會者必須在「適切」的技術難度中，幫助更多關係者理解數位身分（digital identity）的概念，因為技術過於困難，相關概念往往對於網路使用者很重要，但是對於大眾而言又過於難以理解。同時數位身分生態系缺乏同業公會也被認為是一個產業困境，目前全球相關產業都還在初期階段，市場規模小，相關新興技術、新興標準尚仰賴非營利組織運作，頗有網路建構初期的樣貌。在此整理一些相關

生態系，與會者使用 Liminal 有關數位身分的產業報告地圖進行分析，如圖所示，綠色色塊為新興科技與新興產業，網路身分工作坊作為相關技術的領先會議，主要集中在右邊三個綠色色塊，分別為「數位皮夾/身分錢包」、「電子身分與公民身分」、「去中心身分與可驗證憑證管理」等。



圖 9、與會者使用 Liminal 有關數位身分的產業報告地圖進行分析¹³（來源：Liminal Links）

以下初步整理目前既存有關分散式身分與可驗證憑證的國際組織，與其關係網路。第一大類為 Linux 系列基金會，包含分散式身分基金會（DIF）、超級帳本基金會（Hyperledger）與最新的開放皮夾基金會（OWF），只要是基於 Linux 精神營運的基金會，都是擁抱自由軟體（Open-Source Software）的組織，這三個組織於不同時間點成立，處理不

¹³ <https://link.liminal.co/solution-segments>

同議題，分別為如何讓分散式識別符彼此互通、區塊鏈如何成為可信任網路的具體服務（Hyperledger 以聯盟鏈精神進行運作，如今被許多企業級解決方案所使用，臺灣的福爾摩沙鏈、司法聯盟鏈也使用相關技術，不過 Hyperledger 本身也有許多新興專案正在運作）、與開放原始碼並可以互通的數位身分皮夾服務，其中 OWF 支持的 Bifold 開源專案目前已與加拿大卑詩省合作，推出 BC Wallet，成為地方政府有關數位身分的領先專案；第二大類為 W3C 內部工作組相關組織，包含分散式識別符工作組（DIDWG）、可驗證憑證工作組（VCWG）與網路孵化社群組（WICG）持續開發的聯邦式憑證管理（Federated Credential Management, FedCM），目前 W3C 持續運作的協力者中，目前開發方向往關聯式資料（LD）與資料可信度（DI）方向進行探索，由於具有開發難度與學術風味，應用性與相容性上備受挑戰，在會中卑詩省相關開發團隊分享了他們如何使用 Hyperledger 衍生技術 Annocreds 實現了與 W3C 可驗證憑證資料模型（VCDM）互通的案例（見附錄 5¹⁴）；此外自從可驗證憑證（VC）概念被提出以來，又有許多標準組織近一步提出了相關規範，如網際網路工程任務組（IETF）提出 SD-JWT VC 概念，朝向選擇性揭露相容性進行開發，相關組織也包含開放身分基金會（OpenID），過去提出 OpenID1.0、OpenID2.0、OpenID Connect 等標準，實現了單一簽入（SSO）功能。該基金會目前進一步提出有關可驗證憑證、展示、提供者的相關標準，如 OID4VC¹⁵、OID4VP¹⁶、SIOPv2¹⁷等草案，以上標準制定者多數曾在 W3C 組織服務，如今轉向更具有彈性的 SDO，同時繼續支援分散式身分與可驗證憑證生態系標準層次的維護，目前這些標準也

¹⁴ 附錄 5、20240418 BC Gov CWU_ AnonCreds in W3C VCDM Format

¹⁵ <https://openid.net/sg/openid4vc/>

¹⁶ https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

¹⁷ <https://identity.foundation/did-siop/>

被歐盟數位皮夾相關架構給涵納其中。此外，與美國政府較為靠近的標準組織包含國際標準組織（ISO）所提出的 ISO18013-5、ISO18013-7、與 ISO23220 等，由 ISO/IEC JTC 1/SC 17 技術委員會¹⁸所提供，其標準針對政府發行的行動駕照、電子文件與其互通傳輸原則進行標準制定，在設計上雖然也有隱私保護與反追蹤等設計，但在精神上與分散式身分相對遙遠，目前許多行動裝置相關的作業系統廠商，在皮夾相關業務上，以符合 ISO 標準為主，這是因為 ISO 與美國國家標準暨技術研究院（NIST）、國土安全部（DHS）長期保持密切合作關係，在技術成熟度上也較高。此外如前文所述，同樣也是 Linux 基金會旗下的超越網際網路信任協定之信任架構基金會（Trust over IP Foundation）是在網路基礎架構下，重新討論數位身分之治理與技術堆疊（Stack）如何實現的重要組織。最後，有關數位身分的區域級或產業型組織也包含推進數位身分的 IDPRO、加拿大數位身分認證委員會（Digital ID & Authentication Council of Canada, DIACC）、非洲身分（ID for Africa）、歐盟區塊鏈服務基礎架構（EBSI）、探討快速登入與行動密鑰標準的 FIDO Alliance、全球可驗證身分網絡（Global Assured Identity Network, GAIN）、全球法人識別符基金會（Global Legal Entity Identifier Foundation, GLEIF）、開放身分交換組織（The Open Identity Exchange, OIX）等。這些組織與聯合國相關組織如發展署（UNDP）、兒童基金會（UNICEF）、國際飛航組織或 G20 都曾有合作專案，或是更多有關分散式身分之新創企業與大型平台內部創新專案。

第二個參與議程對於網路身分的高階（high-level）原則進行辯證，自 94 年微軟的金·卡麥隆（Kim Cameron）提出《身分法則》（laws of identity）以來，二十年來不斷有機構與思想領袖在相關領域提供修改版本，

¹⁸ <https://www.iso.org/committee/45144.html>

如克里斯多福·艾倫（Christopher Allen）於 2016 年討論有關數位身分自主（SSI）之後，相關概念便更加明確，此外曾提出相關定義的組織也包含世界銀行（World Bank）、世界經濟論壇（World Economic Forum, WEF）、Access Now、The ID2020 Alliance 等組織，在此僅將相關概念條列整理為十條，分別為「包容性：身分應該對所有人開放」（Inclusion: Identity should be available to all）、「控制權：使用者必須掌握自己的身分」（Control: Users must control their own identities）、「存取：用戶必須能夠存取自己的資料」（Access: Users must have access to their own data）、「透明度：系統和治理必須透明」（Transparency: Systems and governance must be transparent）、「持續性：身分必須長期存在」（Persistence: Identities must be long-lived）、「可攜性：身分資料和服務必須可轉移」（Portability: Identity information and services must be transportable）、「互通性：身分應盡可能廣泛可用」（Interoperability: Identities should be as widely usable as possible）、「知情同意：使用者必須同意他們的身分或資料被使用」（Consent: Users must agree to the use of their identity or data）、「最小化：身分資料的揭露必須最小化」（Minimization: Disclosure of identity information must be minimized）、「保護：必須保護使用者的隱私權」（Protection: Users' right to privacy must be protected）等¹⁹。而在開放身分基金會所釋出的《為政策制定者所寫的以人為本的數位身分》白皮書部分，第一部分探討了數位身分技術的機會和風險，任何國家擁抱數位身分都有不同的原因，如經濟誘因、社會公共服務的便利性或國家安全需求等等。第二部分，白皮書分析了不同市場中的數位身分模式，並討論常見

¹⁹ <https://www.newamerica.org/future-land-housing/reports/nail-finds-hammer/the-principles-of-self-sovereign-identity/>

的決策路徑。該白皮書也引用了另一份白皮書《政府發行的數位憑證與隱私景觀》（*Government-Issued Digital Credentials and the Privacy Landscape, Flanagan, 2023*），該白皮書深入探討全球尺度的隱私強化技術相關之數位身分現況所面臨的挑戰。第三部分建立在現有身分原則的基礎上進行治理建議（如上述原則），以幫助政府官員進行決策。該論文認為每一個國家皆有自己的脈絡，相關數位身分政策應因地制宜，沒有一種技術或架構將成為所有國家的最佳模式。因此多元系統將共存並立，而且單一司法管轄區中可能存在多種樣態的數位身分系統。最終該文章還探討了全球數位身分公共建設的可能性，使所有人都能夠在近場與遠端主張自己的身分，同時尊重國內主權。

其中一個議程討論「模組化開放原始碼身分平台」（*Modular Open Source Identity Platform, MOSIP*），MOSIP 是一個主要由發展中國家所使用的模組化數位身分平台，衍生自印度的 Aadhaar 平台。MOSIP 成立的原因是解決發展中國家（主要是南半球國家）由於數位身分服務被壟斷而造成預算上漲，無法使用的問題，目標在於解決全球南方缺乏身分公共建設的窘境。透過 MOSIP 服務使用者互相合作，MOSIP 最後將建立聯邦式的身分生態系，目前共有如摩洛哥、菲律賓、斯里蘭卡、幾內亞、多哥、尼日爾、烏干達、衣索比亞、布吉納法索、馬達加斯加和獅子山共和國等國家使用相關服務。詳情可見 Kaliya Young 於 *Identity Women Business* 所撰寫之「MOSIP，在全球南方不可忽視的力量」（*MOSIP, the Unneglectable Force in the Global South*）²⁰，此外有關印度數位身分系統的深入討論，也可參考《追求證明：印度身分證明文件的歷史》（*In Pursuit of Proof: A History of*

²⁰ <https://medium.com/@identitywoman-in-business/mosip-the-unneglectable-force-in-the-global-south-a7866535b46e>

Identification Documents in India) 一書。



圖 10、圖為 MOSIP 數位身分模組架構圖（來源 MOSIP 官方網站）

關於「超越網際網路信任協定之信任架構」(Trust over IP, ToIP) 議程部分由該基金會參與者介紹近期的工作進度。ToIP 基金會是 Linux Foundation 旗下的獨立組織之一，成立目標在於解決網路基礎建設中缺乏「網路身分層」的困擾。根據該基金會網頁表明「數位經濟必須以信任為基礎，若使用者在網路世界中信任越大，其經濟規模就會越大。但目前個人隱私並不那麼令人滿意，許多人認為個人資料散落在網路中是令人不適的，而且我們並不容易相信他人的數位身分，因而也不會輕易相信內容。」因此 ToIP 基金會以「推動全球標準，建立各方之間的機敏資訊直接連接」、「推動可互通的數位皮夾和憑證」、「使用可驗證數位簽章保護公民和企業身分」、「整合數位信任的技術要素與人的要素——在成功的數位信任生態系統中制定規則和政策」、「促進數位信任專家之間的溝通和知識共享」。該組織除了概念性的白皮書之外，也實作了許多開放原始碼的套件，如 did:web 方法建立、數位信任治理架構技術文件 (Governance Architecture Specification V1.0)、以及前章節所述之金鑰事件收據基礎建設 (Key Event Receipt Infrastructure, KERI) 技術文件等。

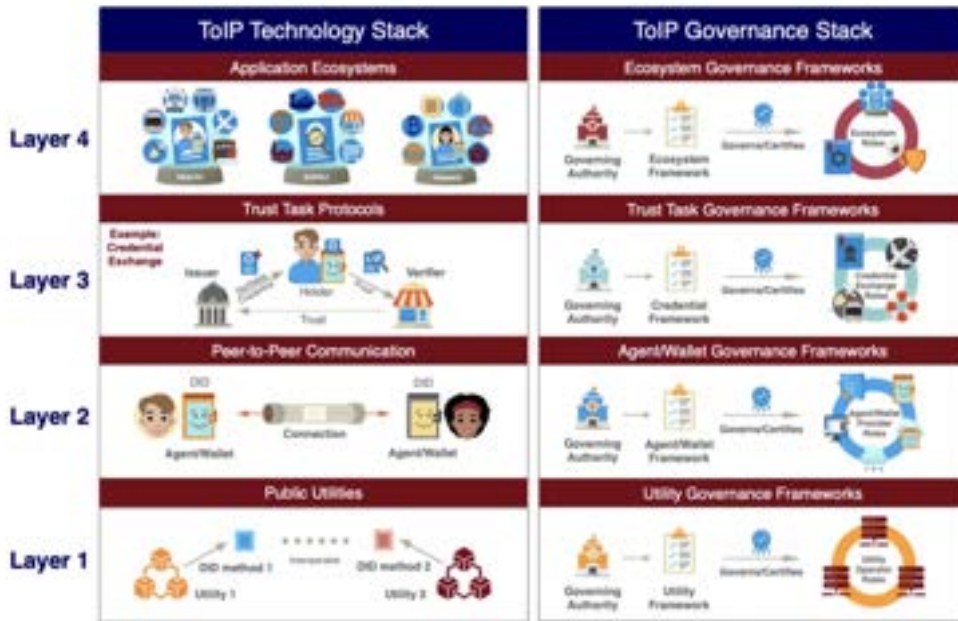


圖 11、ToIP 的官方網頁互動頁面，描繪了 ToIP 在網路不同層次的技術集與治理集（來源：ToIP 基金會官方網站）

在「SSI?VCs Not Dead (yet) : Hot takes and lessons learned from assi/VCs Consulting」場次中，來自 Identity Women Business 的 Kaliya Young 就數位身分顧問的經驗就關數位身分生態系進行討論，深入探討了 SSI/VC（數位身分自主/可驗證憑證）相關社群面臨的複雜挑戰，尤其是在理解使用者思維運作和新興技術發展之間，開發者與使用者之間有一段鴻溝，而且市場還無法讓這樣的題目穩定運作。他們認為開發者社群無法有效傳達與新興技術相關的想法和概念時，讓普通人可以理解。儘管社群內有許多聰明人士，但似乎更傾向於在展示中表達過多想法，而不是專心於有效地傳達好故事。這導致創新者與其受眾之間脫節，阻礙科技，尤其是對於一般使用者而言很重要的科技被廣泛採用的機會。此外 Kaliya 以 Good Health Pass Collaborative 為案例討論疫苗憑證的發展史。儘管該專案框架本身很複雜，但從專案進程中我們可以發現執行單位透過簡化健康證書的基礎架構，最終實現更廣泛的易用性此外，本環節也討論了社群在理解資金與資本流動

及其產業影響方面所面臨的困境。比如歐盟有關數位身分的立法框架（eIDAS 2.0）確定之後，有機會為整個生態系注入資源。本環節的結論是開發者應更有效的面向產業、使用者與政策制定者，才有機會讓整個生態系建立起來。

五、參與第 38 屆網路身分工作坊第三日

於第三日議程中，我們更積極地與不同政府專案相關人員討論數位皮夾的推動，包含加拿大卑詩省推出的 **BC Wallet** 與德國數位皮夾相關的創新競賽，兩者目前都與開放皮夾基金會有深度合作。目前全球各地政府針對數位身分政策推廣，可以分為兩大陣營，一為相對中心化（或聯邦式）的推進路線，將既有的國家級證件數位化之後，放入具有獨有專賣（**proprietary**）色彩的大型供應商所提供的便利服務中，目前美國、日本、澳洲以這個方向為主；另一為擁抱公共程式願景，推動分散式身分（或識別符）與相關憑證標準建立，一方面處理以政府為出發的身分憑證，另一方面也促進產業生態系發展，目前如義大利數位皮夾、不丹數位皮夾等以這個方向為主。另外也有不少國家兼容這兩個路線，譬如韓國的行動駕照放入未公開的區塊鏈中保存、新加坡的數位身分試圖以零知識證明方法強化個人隱私等。這兩種路線都以資料最小化（**data minimization**）、隱私強化技術、電子簽章與抗量子加密方向前進，但其公共服務的推進方式全然不同，分別基於「政府服務數位轉型」與「網路技術架構原生」兩條道路向前。此次我們關注的是擁抱分散式身分的主權國家如何在這個時間點推出方案。

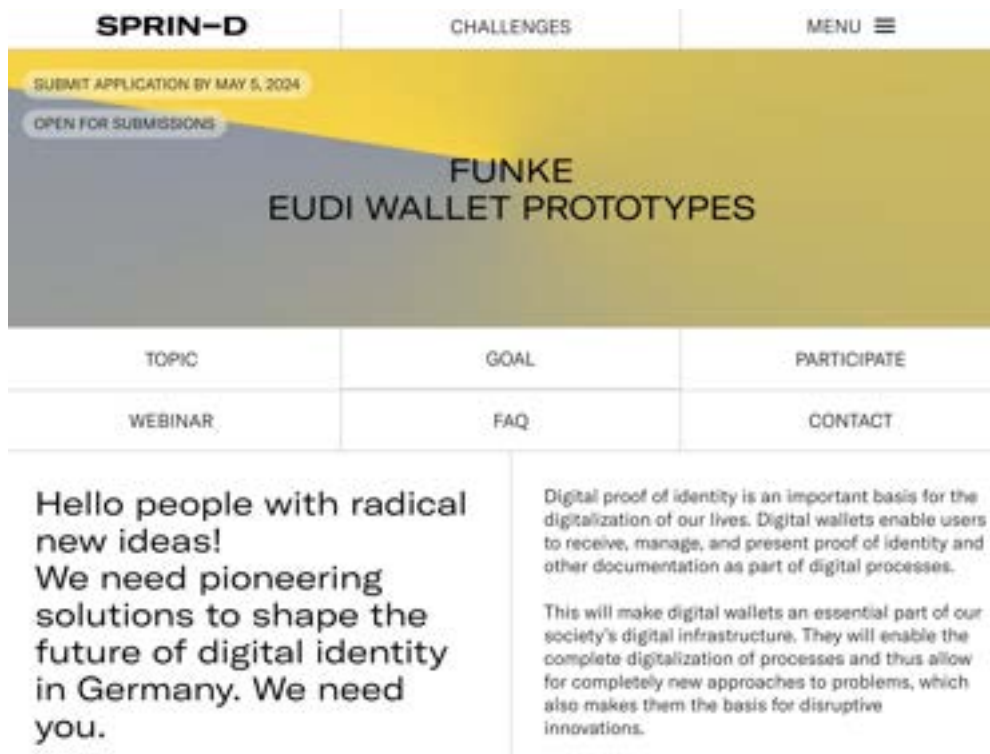


圖 12、圖為德國 SPRIND 總署目前正在執行中的數位皮夾設計競賽頁面

(來源：SPIN-D 官方網站)

德國發表了他們在數位皮夾有關的進度，尤其是在 eIDAS2.0 通過以後，其中一個正在進行中的重要方案為「歐盟數位皮夾原型創新火花競賽」(Innovation Competition Funke EUDI Wallet Prototypes)，這個競賽由德國破壞創新聯邦總署 (Federal Agency for Disruptive Innovation, SPRIND) 執行。其競賽目的為「數位皮夾創造使公民和組織未來得以在數位身分上進行驗證，並以電子形式儲存、管理和展示其個人資料和官方文件。」根據其內政部部长 Nancy Faeser 表示：「透過歐盟數位皮夾，我們正在為德國和歐洲的國家和經濟打造數位未來的基礎。啟動創新競賽是德國數位身分公共建設發展的重要里程碑。由破壞性創新聯邦總署所設計的競賽形式確保將開發出使用者友善和可信賴的解決方案。如此一來，不僅會讓公民更容易與政府機構聯繫，還將在日常生活中帶來顯著的改善—比如網路銀行、求職申請到電子處方籤等等。」該競賽總獎金共 950,000 歐元 (折合新台幣三

千兩百萬左右)。根據講者簡述，不同的團隊可以驗證他們的解決方案，優缺點若被認可，最好的兩個團隊將協助大型數位皮夾試點計畫 POTENTIAL 進行歐盟範圍的皮夾測試。最多會有六個團隊基於皮夾應用的架構概念打造原型服務。每個團隊將至少開發一個 Android 或 iOS 的應用程式。創新競賽的目標是打造一個安全可靠的數位皮夾，使其夠好用，並支援各種手機。創新競賽分為三個階段，在第一階段中，至少要採取一種基於數位皮夾的身分證明設計，類似於德國發行的身分證。團隊可以參考目前歐盟已公布的架構參考框架進行設計²¹，也可以提出自己的想法，只要符合安全、個人資料保護和可互通性的要求即可；第二階段以足夠好用且普遍服務為主，譬如用於管理的數位證書，目標是對所有類型的數位文件（如駕照、居留證、教師證或會員卡）提供全面相容，第二階段的目標是讓紙本文件數位化，以此作為國家數位轉型的基盤服務；最後一個階段也就是第三階段，皮夾原型服務將擴張到登入功能，並允許使用者以匿名方式登錄網站和應用程式。「歐盟數位皮夾原型創新火花競賽」獲得與會者好評並積極討論，我們也與該競賽的主辦者，同時也是德國數位皮夾負責人暨架構師 Torsten Lodderstedt 進行交流，他們歡迎臺德就數位皮夾的原型互通潛在可能性進行技術交流。

²¹ <https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline>



圖 13、德國數位皮夾創新競賽分享環節

此外我們也在會中認識到美國猶他州於今年四月通過數位身分進入區塊鏈的法案。猶他州州長斯賓塞·考克斯（Spencer Cox）簽署了 470 號州議案《政府數位可驗證紀錄法案》（Government Digital Verifiable Record Amendments）²²，該議案重點為向分散式身分與可驗證憑證架構提供預算，該法案目標可為憑證採用區塊鏈技術打開法制框架的可行性。猶他州已經就既有的行動駕照進行試點計劃，該州州民輿論上基於隱私與個人資料保護問題，並沒有被青睞。因此可驗證憑證的試點計畫作為替代性方案被推出，目前並不會一次性參採州民的主要證件如駕照，而是以食品衛生合格證書此類「次要」證件為主。

在最後一個議程中，我們與加拿大卑詩省（British Columbia）有關數位皮夾專案的參與者進行討論，卑詩省推出 BC Wallet，目標為為居民（自然人）與企業（法人）提供數位可驗證憑證服務。BC Wallet 的推進歷程非常特別，在執行原則上也與臺灣數位發展部方向類似，值得我們借鏡。首

²² <https://le.utah.gov/~2023/bills/static/HB0470.html>

先卑詩省已有一個公共程式平台，名為 **Code With Us (CWU)**。CWU 類似民主司即將發展的數位工具入口網與公共程式平台 (**code.gov.tw**)，將可開放原始碼的政府服務集中在平台上，此外該政府也設計了彈性的採購合約，讓公民科技社群的貢獻者可以為專案的維護獲得資源，他們解決了採購機制上 (**procurement mechanism**) 的流程。此外 CWU 以數位平台為模式，媒合了「公務員」與「開發者」，各機關公務員可以在 CWU 提案需求，在規模不超過 7 萬加幣的條件下，創立英雄帖，而全球開發者可以撕榜進行開發，並與特定機關公務員進行討論，並迭代自己的原始碼，最後開放讓所有人都可以使用。而 **BC Wallet** 就是在這樣的框架下誕生。

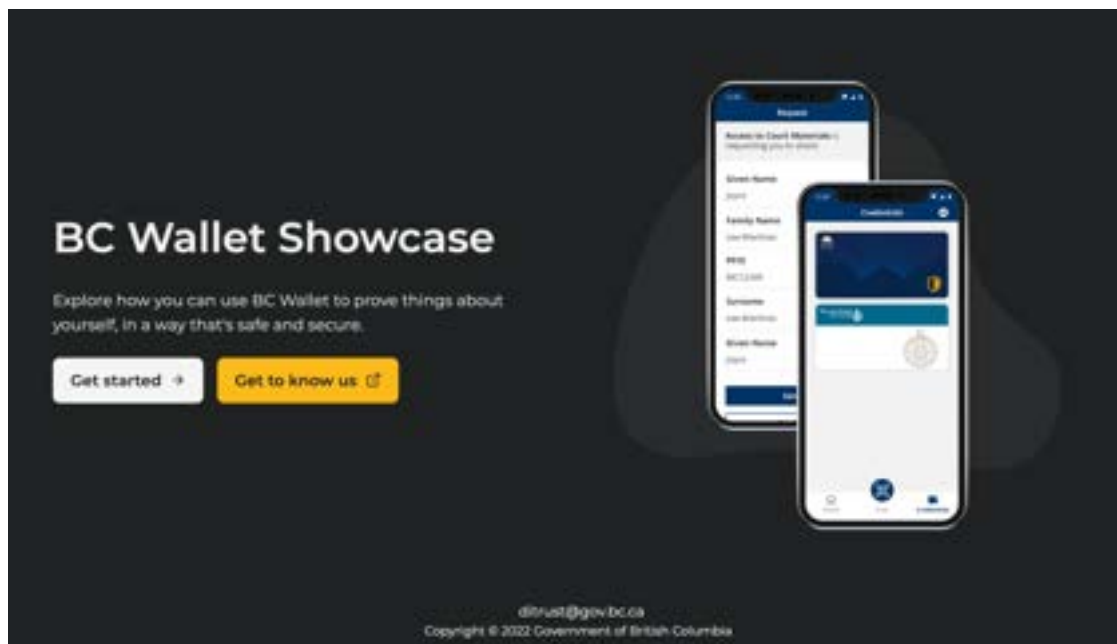


圖 14、卑詩省數位皮夾的動態示範頁面

BC Wallet 使用 **Hyperledger AnonCreds** 標準套件，讓任何人都可以發行符合隱私保護的匿名憑證 (**AnonCreds**) 和可驗證憑證 (**VC**)，並全球資訊網協會所頒布之可驗證憑證資料模型標準 (**W3C VCDM**) 定義格式。在這個專案中卑詩省政府與 **DSR 集團 (Doing Software Right)** 合作，將 **AnonCreds** 成功轉換為 **W3C VC** 格式，而這個套件已經正式開放，讓開放原

始碼社群與政府單位可以直接使用，本次該團隊也有在 IIW 期間進行技術展示。我們認為卑詩省政府將數位治理和數位技術結合，並強化公共服務同時簡化行政流程的模式非常值得我們學習。在數位皮夾方面，它使用 Hyperledger Aries（以發行為主的套件）和 Hyperledger AnonCreds（以驗證保護隱私為主的套件，尤其是零知識證明相關技術），最後成功時做出 BC Wallet 來接收和展示數位憑證。根據分享者資訊，BC Wallet 可以只提供數位憑證中需要的資訊以應對特定情況，也可以證明使用者資料而無需提供具體的文件證明，以上皆滿足選擇性揭露（Selective Disclosure, SD）的需求，這些需求都沒有被定義在目前版本的可驗證憑證標準裡面，也是我們此行欲尋求的解決方案之一。而 BC Wallet 這次以 CWU 模式將 AnonCreds 格式轉換為 W3C VC 與可驗證展示（Verifiable Presentatioin, V）格式，大大的提升了可互通性。

當然目前業界與可驗證憑證有關的解決方案不只是開放原始碼的 Annocreds 方案，目前也有不少套件以開放方式提供不同需求的發行者所使用，在數位皮夾全球生態系發展初期，卑詩省的公開徵求與有效迭代、模組化的建構方式值得學習。

肆、心得與建議：

這次出訪行程是一個極具價值的經驗，對於臺灣分散式身分、數位身分自主權（SSI）與數位皮夾相關數位公共建設計畫之國際合作業務與標準互通進程具有實質進展。在公共建設計畫推行之初進行密切國際交流，證實了臺灣的整體計畫並非空中樓閣，各國實作中的案例提供我們許多令人安心的例證，確立在保護公民的新興科技與網路發展發軔之時，我國數位公建方向並未偏離世界潮流。此外無論是參考各國政府案例，或是理解最新標準草案工作進度，還是以更具體而微的方式理解新興科技發展早期相關產業與大型平台、學術機關、非營利組織互動模式，都令人獲益良多。這些第一手資訊都是在臺灣很難獲取的，藉由主動發表臺灣數位皮夾相關規劃，也獲得了許多國際單位關注，包含美國聯邦政府、州政府、加拿大政府、德國政府與日本相關人士等等，這些交流有助於後續更深入的潛在合作。在參考各國與個組織根據以上現狀，有關數位皮夾或分散式身分相關專案調整的初步建議如下：

一、臺灣數位皮夾應相容之國際標準，並維持彈性的迭代精神：經歷此行，我們理解到國際上有許多標準制定組織其公開之標準都與數位皮夾相關聯，尤其是自全球資訊網協會頒布分散式識別符與可驗證憑證資料模型後，又有更多不同組織標準草案提出，各地也採用不同標準，標準之間可互通需求目前仍尚待工程端解決。這些標準在需求方向上有些許不同，無論是更趨近於中心化的管制風格，還是分散式的開放互通風格，其各有利弊。如何選擇並制定符合臺灣公民需求的標準是當務之急，甚至標準選擇流程的「數位治理」本身便是一個值得妥善設計與公眾溝通的必要專案，我們應回歸具有共識的概念性需求，再根據需求尋找最適合的標準；此外我們也應保持彈性，開發出兼容不同標準可能性的數位皮夾公開套件服務。

二、更積極的參與國際開放皮夾或開放錢包相關倡議與工作網絡，並發展基於憑證互通的國際與全球合作關係：開放、透明的皮夾套件是符合全球公民數位生活的基石，相關精神包含個人資料隱私權、參與計畫的主動性與個人身分自主權。目前數位皮夾規劃草案內容與其相符。開放互通有助於降低國際合作門檻，並有效提升民主網絡的具體成效。除了串聯臺灣內部公私單位發展生態系之外，也應密切注意各地區數位身分與數位皮夾發展趨勢。這是因為目前各國由政府主導的皮夾計畫，尚以試點計畫為主，並逐步擴及不同業務需求與政府服務。本部應主動聯繫試點計劃並交換工作成果經驗，更進一步討論合作的可能性。這是因為有關數位皮夾的政府專案多屬開放精神，且擁抱跨區合作精神，達到全球互通的目的。

三、研議於臺灣辦理國際皮夾議題研討會的可能性：目前相關議題的技術發展單位多以歐美為主，亞太各地目前已有零星成功的試點案例，這些案例經驗與技術交流或可為臺灣正在萌芽的數位憑證與信任科技生態系提供更密切的合作機會，並增加數位公共建設計畫打造公開套件並被密切使用、維護的目的。相關案例可參考泰國經常性舉辦的 APAC Digital Identity unConference（相關議程運作文件詳見註解²³），該活動目標在於促進新興數位身分產業與專案在亞太地區之間合作，並邀集多方關係人參與，達到相關服務可互通的目的。該活動的辦理方式來自於本次參與的網路身分工作坊（IIW）。經內部研究指出，臺灣目前有關信任科技與數位皮夾相關關係人多為新創企業、學術單位等，大型產業生態系尚未萌芽，且國內尤為缺乏參與國際事務的標準建構者，舉辦相關會議或可促進該議題發展，提升智慧國家的進程。

四、研析我國「集中化—分散式」數位憑證服務方向：從數位轉型的觀

²³ <https://cdn-assets.inwink.com/5b73d46b-329d-44a2-a4b7-eb92bf54c4c1/e6c2bcca-c933-4663-86b8-42ed0fe05e6f>

點，有關數位皮夾相關的公共服務，可展開為「集中化—分散式」光譜，集中式數位身分往往與電子化政府脈絡一致，此方向可以英美體系國家為主，延伸到印度與一些發展中國家；而分散式身分與新一代的數位自主權靠齊，以歐陸體系做為代表，根據多國聯合法制基礎的布魯塞爾效應（Brussel Effect）影響，歐洲「第二代電子化身分認證與信任服務」（eIDAS）於 113 年 3 月初通過立法程序，確立了分散式身分與數位皮夾的法源依據，也從一開始將大型平台的錢包服務如 Apple Wallet、Google Wallet、Samsung Wallet 限制到不可能獨霸的狀態。集中式身分解決方案恐以主權國家與大型跨境廠商合作為方針作結。回到「集中化—分散式」光譜，以上兩者並非涇渭分明，事實上此間尚有許多兼而有之的國際案例，如前章節所述。集中與分散與否並不代表歷史脈絡是一成不變的，國家政策會轉向，技術架構數十年來也經歷許多輪別的顛覆創新。過去發行身分證的國家，不一定未來就會自然而然地發行數位身分證；同理，過去沒有身分證的國家，不代表未來就不會有集中式的身分數位證件，比如過去相對分散，僅發行駕照與社會安全碼的美國聯邦政府與州政府正在一步步地往集中方向靠攏，從 89 年代反恐政策的 Real ID 開始一路到現在的行動駕照標準（mobile Driver License, mDL），各州雖仍維持一定的獨立性，但聯邦級機關與企業體正在慢慢整合各州標準，目前蘋果與谷歌等作業系統服務商已可將不同州別的駕照或州民證用來搭國內航班，以上案例為與美國運輸安全管理局（Transportation Security Administration, TSA）積極合作的結果。日本是另一個值得參考的案例。日本的數位廳（Digital Agency）比臺灣的數位發展部早三年成立，其中一項重點政策就是個人編號卡（My Number Card），日本在過去是沒有身分證的，進行有關身分的證明通常是一頁 A4 紙，有鑒於此，日本推出了有 IC 晶片卡的個人編號卡來解決數位轉型的問題，目前約有九千多萬人申請。當然，個人編號卡類似於臺灣過去曾欲進行的數位身分證（eID）專案，此

間也有許多個人資料保護、個人隱私相關的論證。到了民國 111 年，日本首相岸田文雄直接公開問蘋果 CEO 庫克（Tim Cook）能否協助將個人編號卡放入 Apple Wallet，庫克的回應是希望日本政府先解決隱私與知情同意（Informed Consent）的問題。由此可知，日本正在藉由大型平台之力整合集中式數位身分服務，日本選擇了便利的公民服務這條路。但是同一時間日本也有關於分散式身分的努力，數位廳（Digital Agency）的研究報告也有分散式身分與數位皮夾相關規劃，譬如日本在打造信任網（Trusted Web）上持續發展，該研究組今年花了約莫台幣一千多萬元費用委託凸版印刷株式會社與 Panasonic 執行了日本數位皮夾原型驗證案（JP-DIW PoC）。此外數位廳另一個研究組「web3 研究組」也正在進行有關分散式身分與可驗證憑證（DID/VCS）體系的研究，而日本自民黨（FDP）於 113 年 4 月提出最新版本的 web3 2024 白皮書，又再次提到了分散式身分是日本進行數位轉型（Dx）的一大基石。在如此多線並行的狀況下，日本在數位身分會走向何方有待觀察。在 IIW 會中與 OpenID 基金會的執行長崎村夏彥（Nat Sakimura）討論時，他認為日本數位身分的方向也會慢慢朝向集中。他在甫出版的《Web3 の未解決問題》書籍中主寫「『分散』と『集中』をめぐる歴史」，簡介 DID 的歷史流變。

即使如此，許多國家正在最大化可互通性為目標，尤其是日趨重要的數位憑證與可驗證憑證等。因此以公共服務而言，數位身分或數位憑證的發行將是各國政府接下來的重要業務，如何達到公民自決，善盡資料保護的精神，乃是目前最急迫需要處理的問題，相信分散式的解決方案是符合世界趨勢的方向。

Digital Innovation Key Infrastructure Project –
Taiwan DID Wallet Authentication Module System Development Project

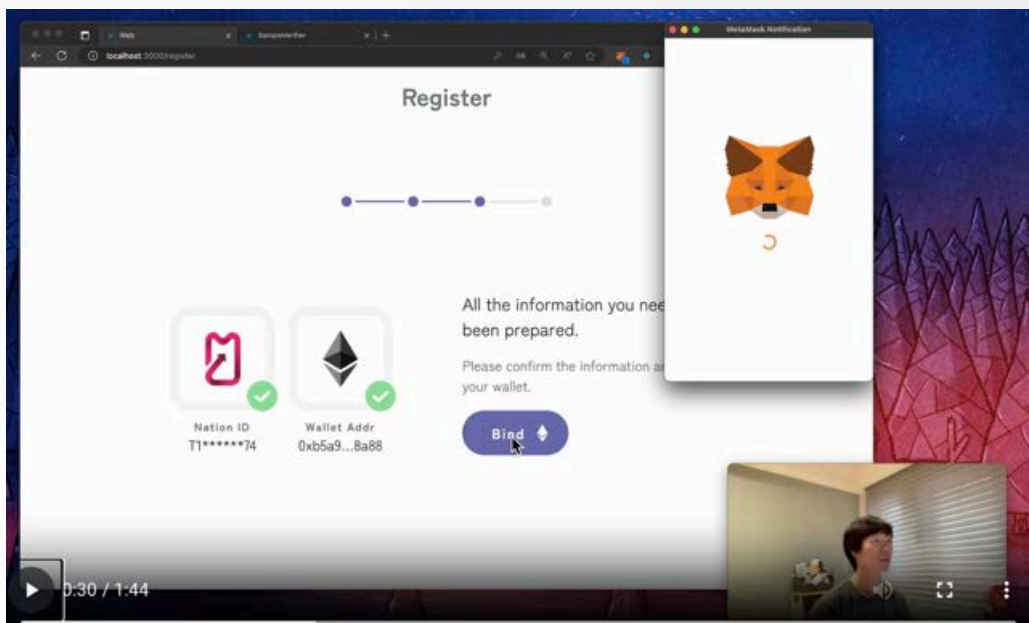
DID Wallet Draft Introduction



Ministry of Digital Affairs
Department of Democracy Network
web3 architect, mashbean
2024.03 CC0

This presentation content is for reference only. For detailed information,
please refer to the information provided on the official website of the Ministry of Digital Affairs.

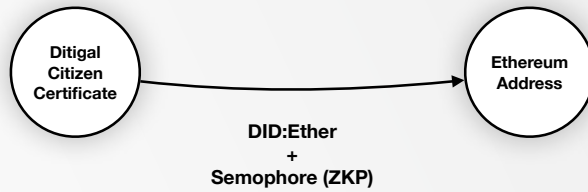
1



2023 PoC Project: TW-DID

<https://github.com/moda-gov-tw/tw-did/releases>

2



Proof of Personhood

2023 PoC Project: TW-DID

<https://github.com/moda-gov-tw/tw-did/releases>

3

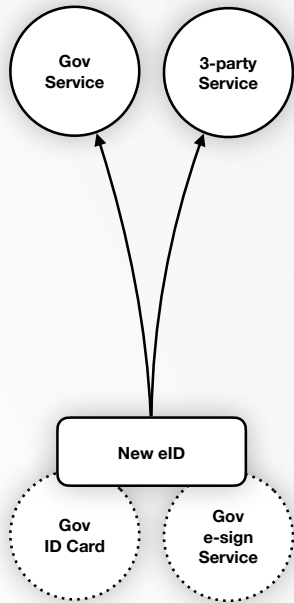
2024–2027 Taiwan DID Wallet Project

Digital wallet refers to international standards,
 Establishing the verification infrastructure
 for a digital democratic society;
 Guarding personal data and privacy,
 Achieving personal digital autonomy,
 Data authorization and self-determination.

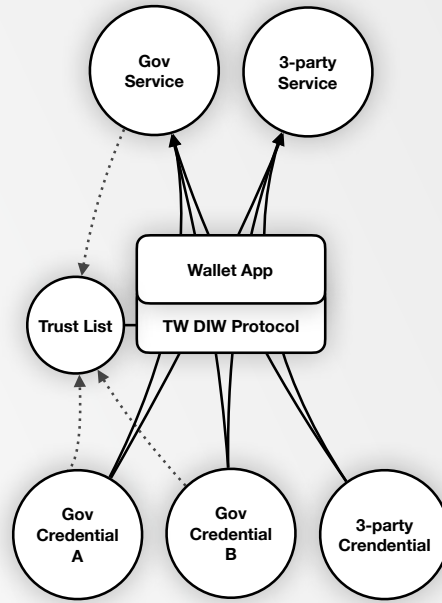
Using international standards:
 Decentralized Identifiers (DIDs v1.0, 2022)
 Verifiable Credential Data Model (VCDM v1.1, 2022)
 published by the World Wide Web Consortium (W3C),



4

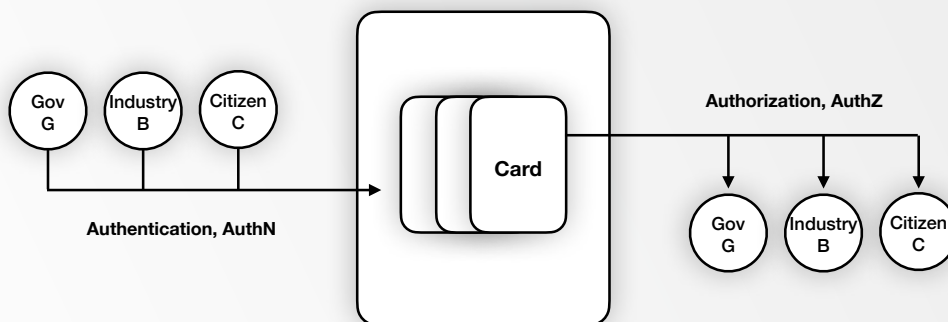


**Taiwan New eID
ID-Based Service**
(Centralised Digital ID System)
was **Suspended** in 2021



**TW DIW
Wallet-Based Service**
(Decentralised ID System)
is a public infrastructure project in 2024

Brief Introduction



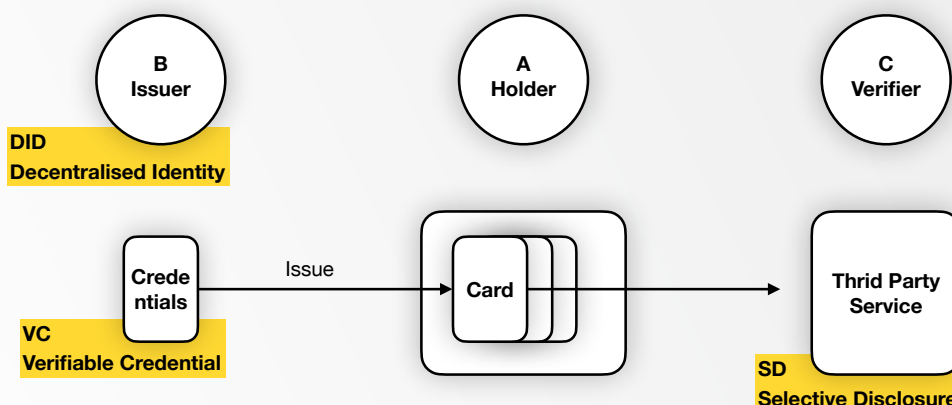
Digital wallets consist of Decentralized Identifiers (DID) and Verifiable Credentials (VC), they are not another eID Program.

High-level Concept

- *De facto* identity
- Self-sovereign identity (SSI)
- Composable & programmable social relationships
- Permissionless & Open-Source
- Interoperability
- Passwordless
- Secure & Privacy Preserving
- Functional Equivalence
- Resilience and Social Recovery
- Opt-in & Opt-out

7

Decentralized Identity/ Verifiable Credentials Triangle

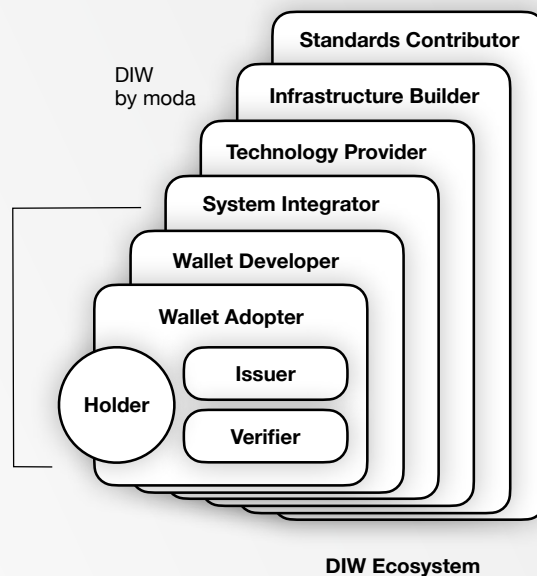


Proposed use of privacy protection measures related to zero-knowledge proofs

Goal: Through nationwide public infrastructure, establish the prerequisite conditions necessary for Taiwan to achieve self-sovereign identity, ultimately leading to a future where citizens' personal data privacy is protected.

8

In Taiwan, software standard development is typically led by the government, with the industry building the relevant ecosystems.



9

Timeline

2024 — 2027

1. **Public Building Blocks:** Open-source packages, cross-department testing, private sector sandbox
2. **Trust Registry:** Maintenance of trusted lists
3. **User Interfaces:** User-end apps and issuance, verification services
4. **Standard Update:** Ongoing updates from technical promotion teams, regulatory adjustments

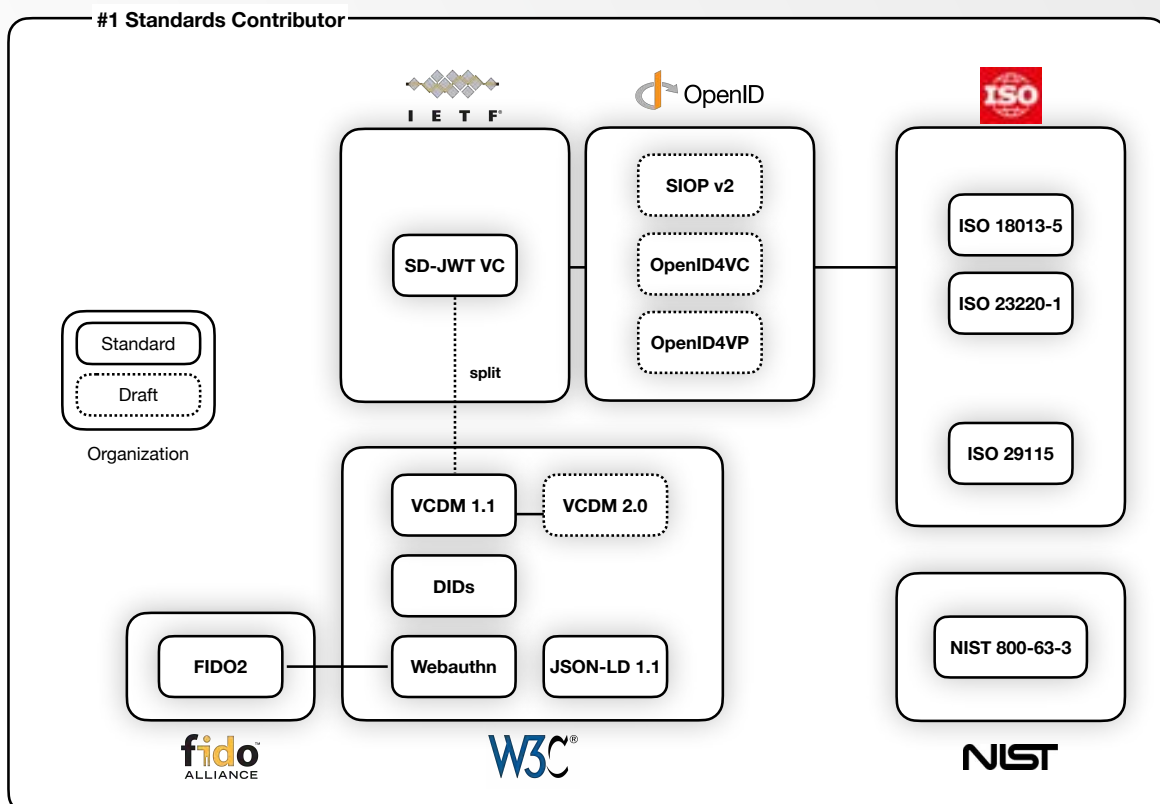
10

Conclusion

1. The digital wallet is **not** a reboot of eID; instead, it enhances the **digital sovereignty** of individuals through "verifiable credentials," allowing individuals to choose whether to use them or not.
2. The digital wallet provides **open-source public service**, offering a set of tools for both public and private sectors for issuance and verification, with the source code available for public review and use.
3. This **public infrastructure project** employs technologies to enhance privacy and security, ensuring the security of users' personal data in various application scenarios.
4. The digital wallet adheres to **international standards**, providing Taiwan's government, industry, academia, and research institutions with a set of public standards, serving as guiding principles for global credential interoperability or domestic recognition.

11

Currently, there is still competition among international SSI standards.



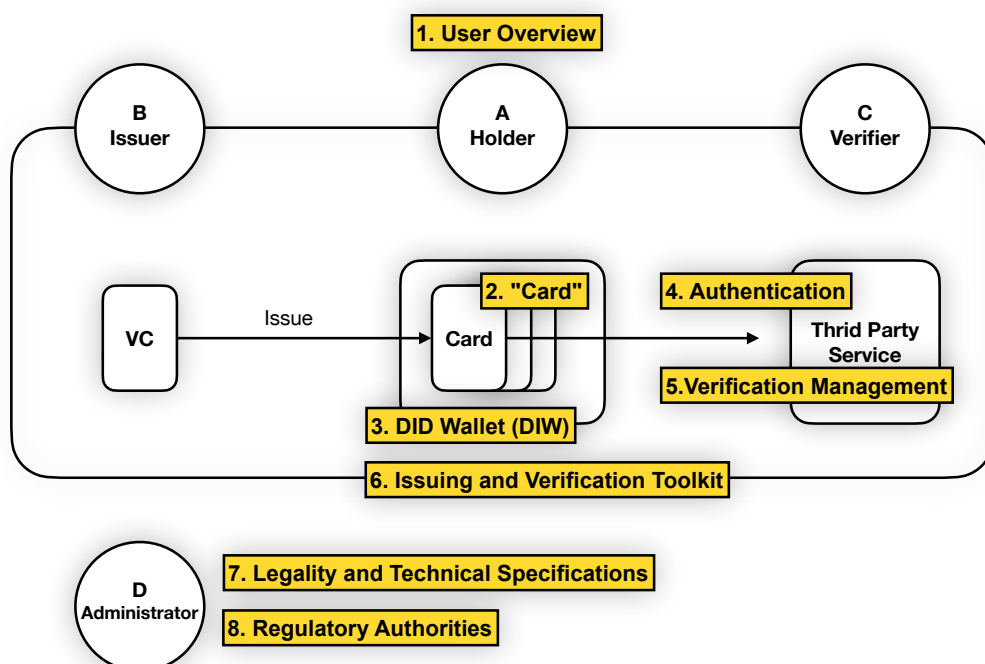
12

DID Wallet

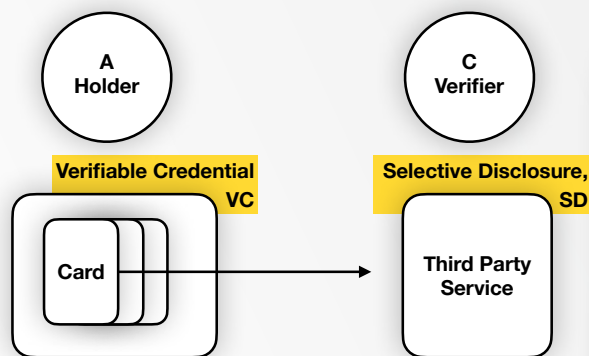
Building a Public Credential Service that Balances Privacy and Convenience

moda

13

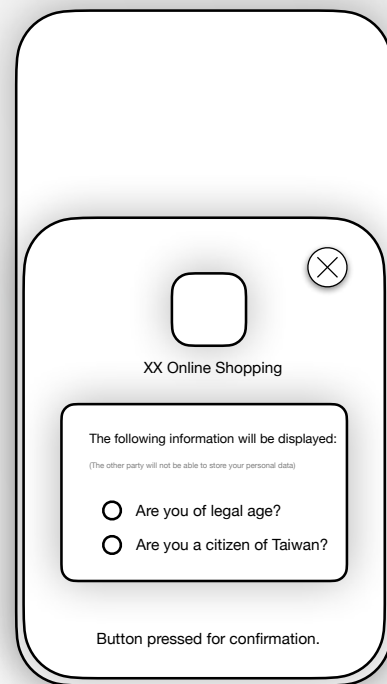


14



Selective Disclosure:

It allows for the verification of qualifications without revealing all information contained in the credential, enabling the verifier to determine if the individual meets the criteria.



Core Objectives of DID Wallets

1. **Citizens:** Build a signature and authentication mechanism that combines privacy and convenience, connecting various digital services to prevent digital footprint problems.
2. **Government:** Provide secure and convenient digitalization solutions for government agencies, accelerating the realization of the smart nation goal and improving digital transformation.
3. **Industry:** Enhance and define more secure and interoperable interface standards, becoming the cornerstone of digital services.
4. **International:** Construct identity interoperability protocols for cross-border recognition, improving the convenience of overseas or digital life for citizens and reducing international identity recognition barriers.

Enabling a trusted digital future

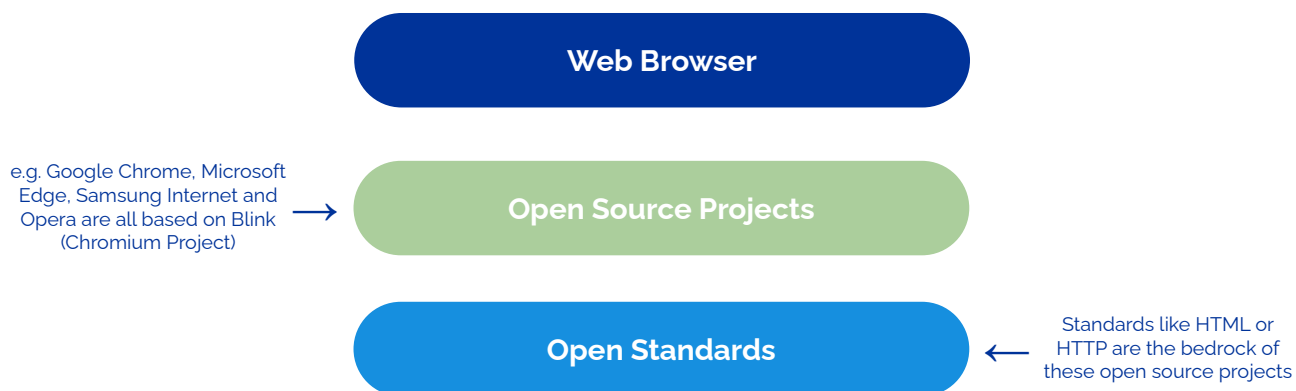
December 18, 2023



Antitrust Policy Notice

- Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.
- Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at www.linuxfoundation.eu/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrave of the firm of Gesmer Updegrave LLP, which provides legal counsel to the Linux Foundation.

Every browser is based on open source code



Why

Because open source development is faster and cheaper and can foster safety and interoperability.

We deploy this model for digital wallets

Digital wallets may hold many credentials e.g. identity, drivers licenses, health, academic, access, crypto assets



Most use cases require adherence to different standards and rules that differ by country



Creating a safe space for all stakeholders

provide funds and nominate board members who decide on the budget



FREE



stay in control of their code and nominate TAC Members who decide on new projects



provides feedback and nominates a board observer



FREE



FREE



nominate GAC members providing feedback to projects

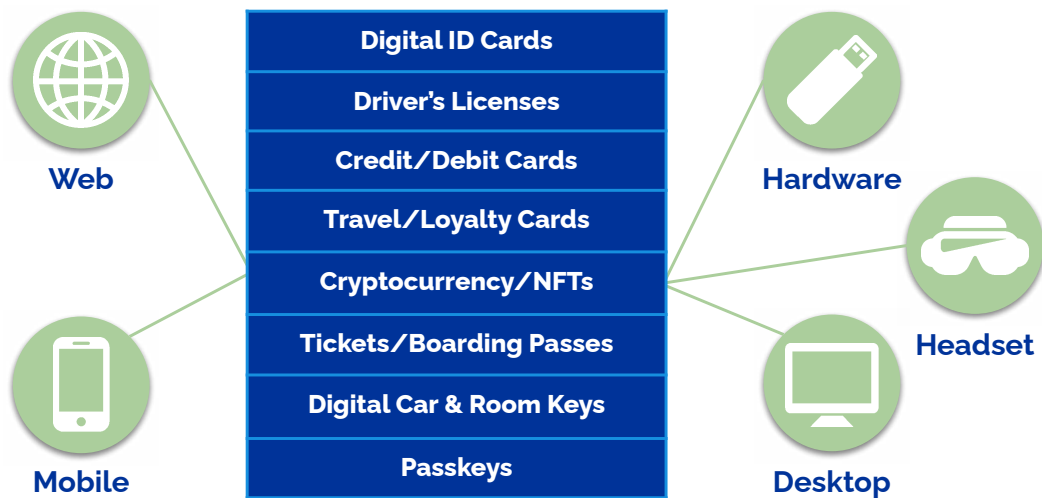




Initial Governmental Advisory Council Participants

- To date, the Governments that have joined the OWF [Governmental Advisory Council](#) (GAC) include the United Kingdom, China, Switzerland, Sweden, Portugal, Papua New Guinea, Mexico, Bhutan, Argentina and United States.
- The GAC Government Representatives' details are available [here](#)
- If you want to learn more about the GAC, don't hesitate to get in touch with the GAC Secretariat at GAC@openwallet.foundation.

Digital Wallets serve many purposes



Current Projects

Project Name	Stage	Approval Date	Short Description
sd-jwt-python	Labs	May 27, 2023	A Python implementation of the Selective Disclosure for JWTs (SD-JWT) specification.
sd-jwt-kotlin	Labs	May 27, 2023	A Kotlin implementation of the Selective Disclosure for JWTs (SD-JWT) specification.
Farmworker Wallet OS	Labs	Aug 9, 2023	Low code components for the Mendix platform that can be used to create digital wallets.
VC-API	Labs	Sep 28, 2023	An implementation of the VC API draft standard in REST that includes operations such as credential issuance, verification, and exchange.
Wallet Framework .NET	Labs	Oct 5, 2023	Multiprotocol wallet framework enabling implementations of OpenID4VC and SD-JWT VC, in accordance to the European Identity Wallet initiative's objectives.
Identity Credential	Labs	Oct 18, 2023	Android libraries and reference applications for working with real-world identity.
sd-jwt-js	Labs	Nov 1, 2023	A JavaScript implementation of the Selective Disclosure for JWTs (SD-JWT) specification.
sd-jwt-rust	Labs	Nov 15, 2023	A Rust implementation of the Selective Disclosure for JWTs (SD-JWT) specification.
sd-jwt-dotnet	Labs	November 29, 2023	A .NET implementation of the Selective Disclosure for JWTs (SD-JWT) specification.
Agent Framework JavaScript	Growth	November 29, 2023	Previously known as Hyperledger Aries Framework Javascript, it initially heavily relied on Hyperledger standards such as DIDComm, Indy, and AnonCreds. However, with advancements in verifiable credential technology and the emergence of new standards, the framework underwent multiple refactoring and modularization processes to maintain interoperability.

What OpenWallet provides to projects

- **Infrastructure (Ry Jones)**
 - project onboarding and support with tools like GitHub, Discord;
 - analysis of contribution data
- **Engagement (David Boswell/Sean Bohan)**
 - raising the profile of projects through workshops, meetups, blogs, events;
 - community building online (Hubspot) and at local and regional levels
- **Strategy (Torsten Lodderstedt)**
 - review of project landscape to foster collaboration and fill gaps
 - move organizations to get involved as maintainers/sponsors in projects they use
- **Collaboration**
 - between Government officials, NGOs (SDOs, Civil Society), companies and developers



Community Meetings

A *special interest group (SIG)* under the Technical Advisory Council (TAC) is a group with a shared interest in advancing a specific area of knowledge, learning, or technology related to the mission of the OpenWallet Foundation where members cooperate to affect or to produce solutions within their particular field.

A *task force* is a group that is focused on a task with limited scope and fixed time to complete. A task force will have a specific set of deliverables or work products that it will create and be limited in time to completion.



Community Meetings

Name	Type	Approval Date	Short Description
Architecture	SIG	Apr 05, 2023	Focused on conversations related to the architecture of digital wallet engines.
Credential Format Comparison	SIG	May 31, 2023	Maintain information about available credential formats for the benefit of OWF projects and the wider community.
Digital Wallets and Agents Overviews	SIG	Sep 20, 2023	Further develop and maintain the Digital Wallet Overview and create a similar overview for digital identity agents/SDKs. These overviews should provide transparency of the characteristics of wallets and agents in order to allow for comparison and effective decision making on which wallet is applicable for your use case.
Safe Wallet	SIG	Sep 20, 2023	Create, distribute and promote a set of material that will become the de-facto way to determine how "safe" the new breed of digital wallets is, and be able to compare them effectively. This will increase the visibility of the solutions to correlation and profiling issues that could be introduced with digital wallet deployments.
OID4VC Due Diligence	Task Force	May 31, 2023	Investigate the specifications belonging to the OID4VC family thoroughly, check the existing implementations, and start the preliminary work for potentially creating/hosting a reference implementation or a framework that can be used by a wider community for application implementations



OpenWallet stakeholders are building an ecosystem where data flows freely to enable user choice, privacy and security



Participation

	OpenWallet Sponsors	Linux Foundation General Members	Governing Board
Premier	EUR 200,000		Dedicated member
General (by number of employees)	EUR 50,000 (>5k) EUR 25,000 (>500) EUR 10,000 (>100) EUR 5,000 (<100)	EUR 20,000 (>5k) EUR 15,000 (500-4999) EUR 10,000 (100-499) EUR 5,000 (<100)	1 member for 10 sponsors
Developers	Free	—	1 member (TAC Chair)
Governments	Free	—	1 observer (GAC Chair)
Community	Free	—	1 observer



**Join the growing list of
organizations enabling a trusted
digital future**

openwallet.foundation

info@openwallet.foundation



Decentralized Identity Foundation (DIF)

Introduction to SSI
IIW Spring 2024

April 16th, 2024



Welcome

Nice to Meet You



Limari Navarrete

Sr Dir Community Engagement
Decentralized Identity Foundation



Steve McCown

Chief Architect @ Anonymo Labs
DIF Steering Committee

What is DIF?

How DIF Accelerates Adoption for “Decentralized Identity” and Related New Developments (e.g. Decentralized Web Nodes)

- 1** Innovate for rapid development of specifications that become standards
- 2** Create software building blocks and tools for identity solutions comprising DIDs and VCs
- 3** Maintain reference, open-source, implementations and stacks, e.g., Veramo

DIF Focus

DIF is an **engineering-driven organization** focused on developing the foundational elements and building blocks necessary to establish an open ecosystem for decentralized identity and support security, privacy, and interoperability between all participants.



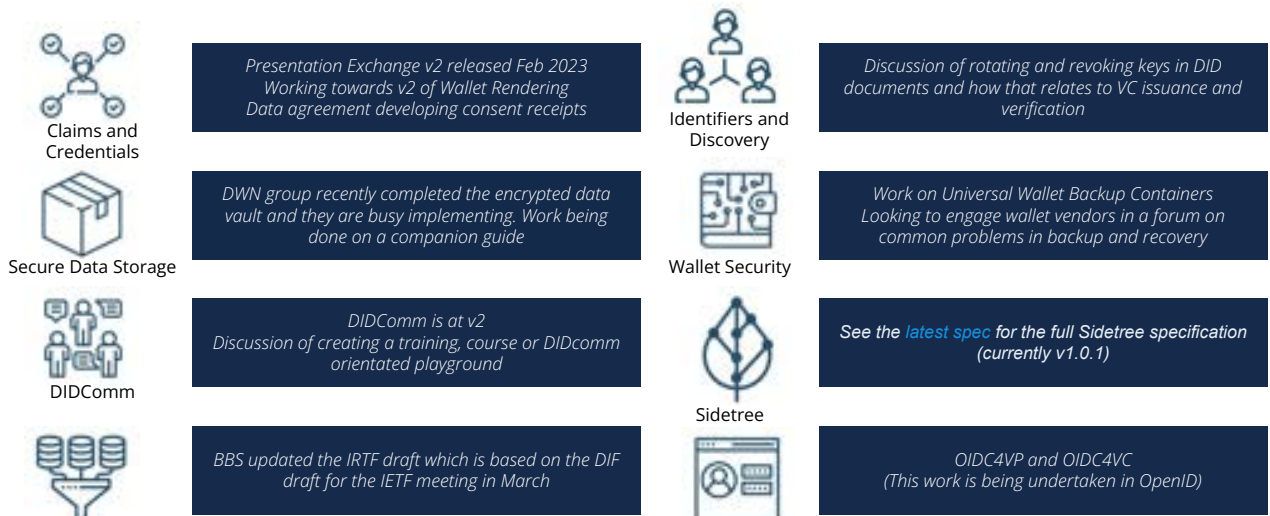
Images: www.flaticon.com



Source: <https://identity.foundation/governance/about>

WG creation policy, <https://github.com/decentralized-identity/org>

DIF Working Groups

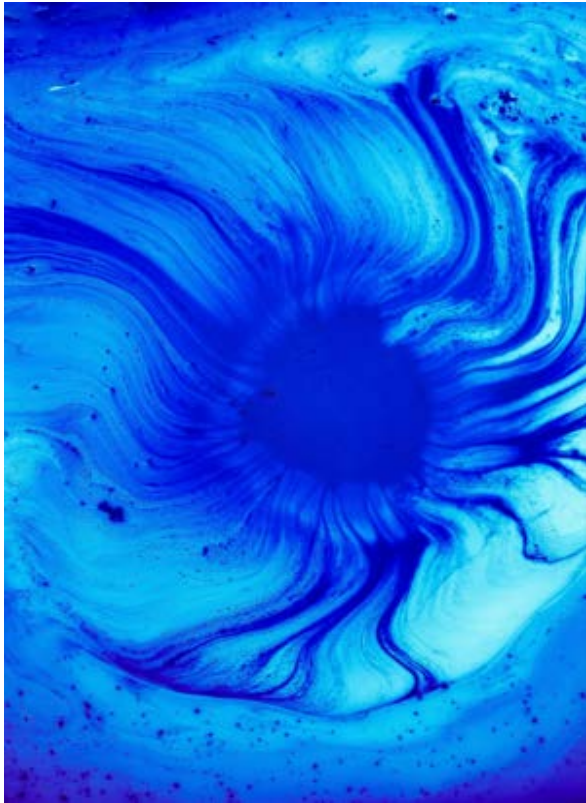


Terms
 IRTF = Internet Research Task Force (long term focus)
 IETF = Internet Engineering Task Force (shorter term, engineering and standards)
 BBS, BBS Signature Scheme, comes from the authors: Boneh, Boyen and Shacham

Terms
 OIDC4VP = OpenID Connect for VP, Verifiable Presentation
 OIDC4VC = OpenID Connect for Verifiable Credentials

DWN = Decentralized Web Nodes, check out the AMA (March 2, 2023) by Daniel Buchner here: <https://www.youtube.com/watch?v=MNXowKcB73E>





SELF - SOVEREIGN IDENTITY

The Movement

Photo by [Joel Filipe](#) on [Unsplash](#)



SSI or Decentralized Identity?

Self-Sovereign Identity - a name commonly used to describe the greater community.

Decentralized Identity - name commonly used to describe the technology based on the principles of this movement.



The Challenge



How I Discovered SSI

Me a long time ago



Alarming Shift in the Internet

All of a sudden everyone was handing over personal information, putting their faith in large tech companies.



Photo by [Kenny Eliason](#) on [Unsplash](#)



Privacy Concerns

Edward Snowden

2013 Interviews in the Guardian

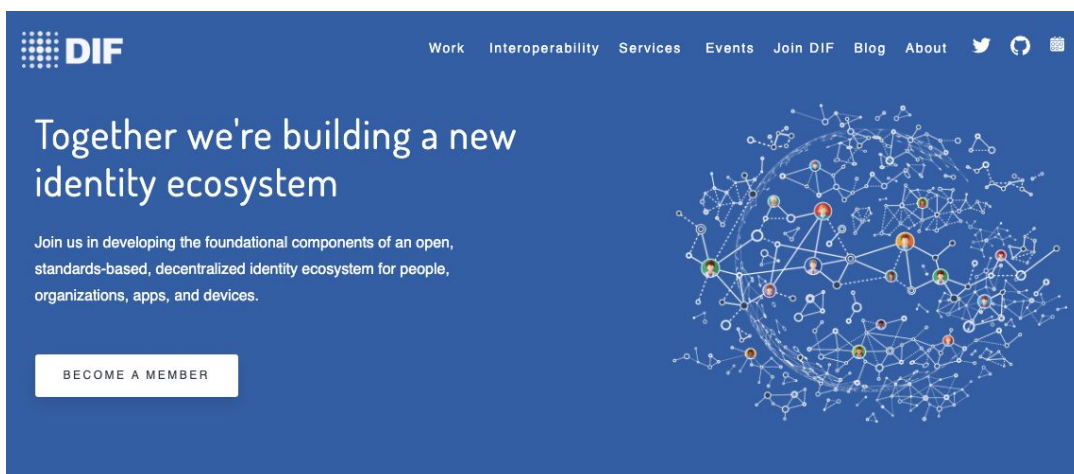


Large Data Breaches

- *Yahoo!* Date: 2013-2016. ...
- *Microsoft*. Date: January 2021. ...
- *First American Financial Corp.* Date: May 2019.
- *Facebook*. Date: April 2021. ...
- *LinkedIn*. Date: April 2021. ...
- *JPMorgan Chase*. Date: June 2014. ...
- *Home Depot*. Date: April 2014. ...
- *MySpace*. Date: June 2013.



I was Introduced to Self-Sovereign Identity



The Origins of SSI



Kim Cameron's Laws of Identity

Microsoft's Chief Architect of Identity from 2004 -2019

"The Internet was built without an Identity Layer"



Kim Cameron's Laws of Identity

Microsoft's Chief Architect of Identity from 2004 -2019

"If we do nothing, we will face rapidly proliferating episodes of theft and deception that will cumulatively erode public trust in the Internet."



Centralized Identity

The model we have used for a long time with all identifiers and credentials

- Passports
- Drivers License
- Facebook login
- Twitter Handle

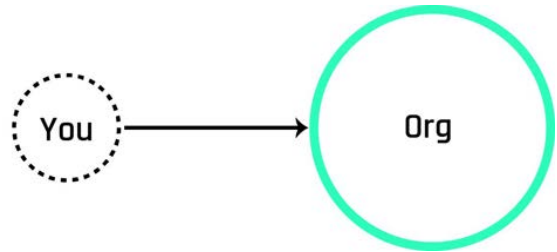
All issued by centralized gvts or service providers

- Every site has its own security requirements
- Your data is not portable and reusable
- Personal databases are honeypots for data breaches

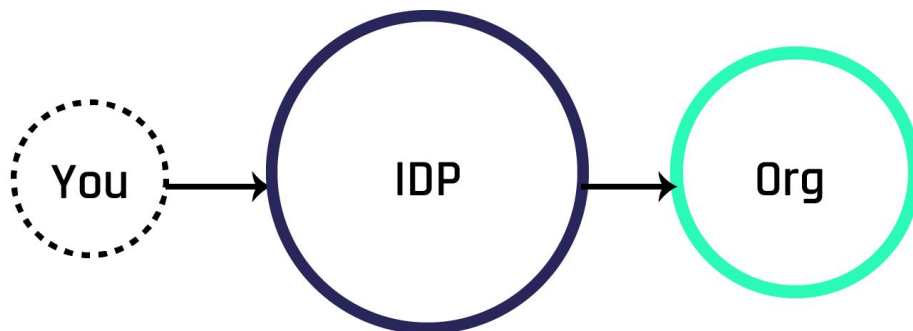


Centralized Identity

At the end of the day those credentials belong to that organization, if you delete all your accounts all the data about you still belongs to that organization.



Federated Identity



Single-Sign On makes the data barons into data emperors.



IIW 2015

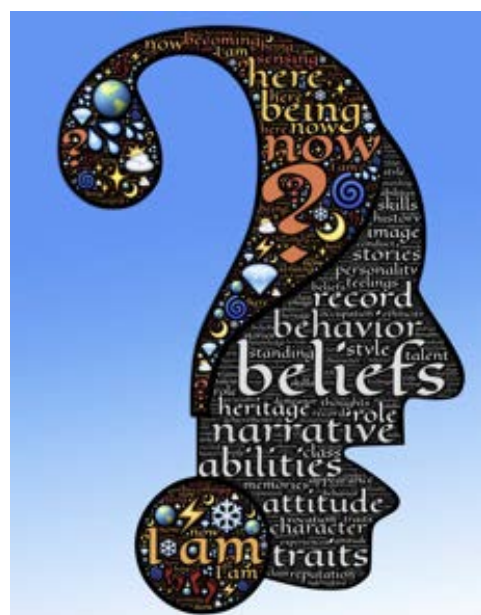
- Blockchain had come to the attention of the internet community
- Several sessions at IIW on “Blockchain Identity”
- US Department of Homeland published a Small Business Innovation Grant Topic Blockchain’s application to identity management
- Other governments follow suit in directing resources in this direction



Laws of Identity

- Written by Christopher Allen in 2016
- A blog post that brought together some of the ideas of various parts of the community including discussions at the W3C as to what are the principles that should govern identity.

<https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/>



Principles of SSI

Existence. *Users must have an independent existence.*

Control. *Users must control their identities.*

Access. *Users must have access to their own data.*

Transparency. *Systems and algorithms must be transparent.*

Persistence. *Identities must be long-lived.*

Portability. *Information and services about identity must be transportable.*

Interoperability. *Identities should be as widely usable as possible.*

Consent. *Users must agree to the use of their identity.*

Minimalization. *Disclosure of claims must be minimized.*

Protection. *The rights of users must be protected.*



SELF - SOVEREIGN IDENTITY

The Technology

Photo by [Pawel Czerwinski](#) on [Unsplash](#)



Tech Foundations

Decentralized Identifiers (DIDs): Digital identifiers self-created by and for people, entities, or things for sharing (publicly or peer-to-peer) public keys and endpoints.

Verifiable Credentials (VCs): Like the paper credentials we use today, but with cryptographic assurances. Enables sharing verifiable data without involving the issuer.

Privacy-preserving Crypto: Cryptographic signatures, end-to-end encryption, and data minimization using selective disclosure, zero knowledge proofs, etc

DID Resolvers: Abstract methods for creating, updating, deleting and resolving DIDs stored in a (too) wide variety of places.

Wallets and Agents:** Applications using data exchange protocols for issuing, holding, and verifying verifiable credentials.

Verifiable Data Registry (VDR): For verifiable credentials, the location where the data needed to verify a credential is found. Any resolvable location accessible to verifiers.



SSI and Blockchains

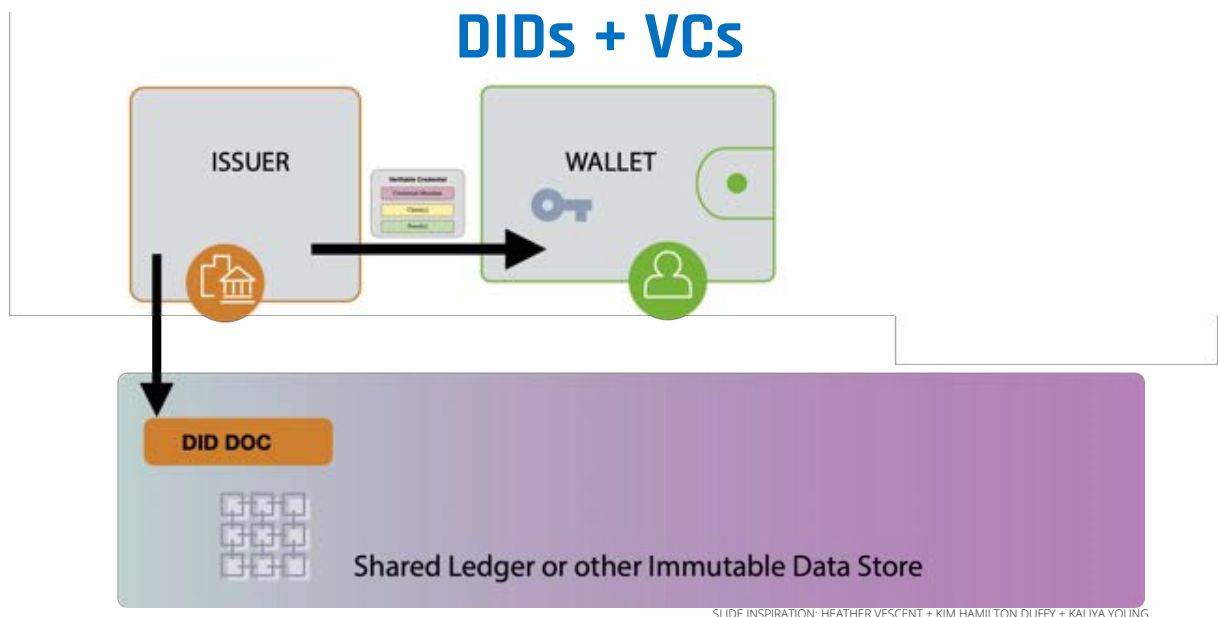
- Blockchains and DLTs aren't perfect, but they're good, stable, production-ready systems for publishing user-managed cryptographic keys at scale.
- Personal data should NEVER be put on a blockchain. SSI is NOT about putting personal data on a blockchain. They are used in SSI for publishing PUBLIC data.
- Blockchain is NOT required for SSI, and DIDs are defined to be agnostic to how and where they are stored.



DIDs + VCs Can...

- Reduce database security risks and business process risks
- Give users more **control** over their identity, data and credentials
- Reduce tracking of user activities, particularly by credential issuers
- Decrease the value of personal information (data from breaches)
- Increase **data portability** and near-global scope (for reputation and history)
- Increase business efficiency through **streamlined onboarding & auditing**
 - Reduce fraud by processing only verifiable data
 - Minimize data sharing to that needed to complete a transaction
 - Streamline confirmation of compliance data/documentation
- **Increase trust** of any data that must be shared downstream

<https://w3c-ccg.github.io/did-primer/>

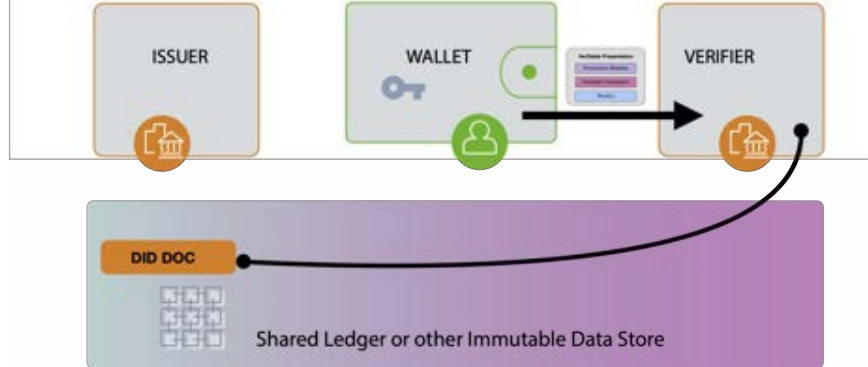


SLIDE INSPIRATION: HEATHER VESCENT + KIM HAMILTON DUFFY + KALIYA YOUNG

- The issuer creates key pairs and a DID, and publishes the DID on a publicly resolvable ledger or other data store. The issuer signs the verifiable credential with the private key corresponding to the one in the DIDDoc, and gives the VC to the holder.



DIDs + VCs



SLIDE INSPIRATION: HEATHER VESCENT + KIM HAMILTON DUFFY + KALIYA YOUNG

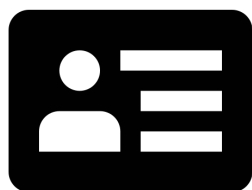
- The Verifier looks up the DIDDoc Of the Issuer and uses the information it contains to check the cryptographic signature from the issuer to know it came from them and has not been tampered with.



What is DID Communication?

Secure, private peer-to-peer messaging

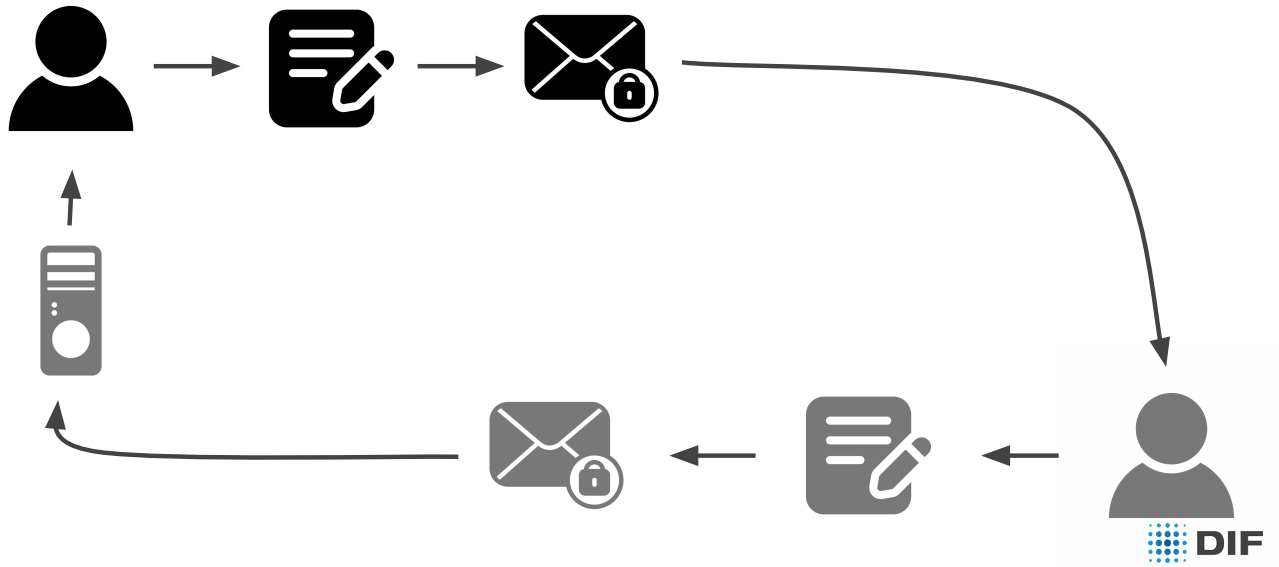
Verifiable Credentials
are **about** the subject



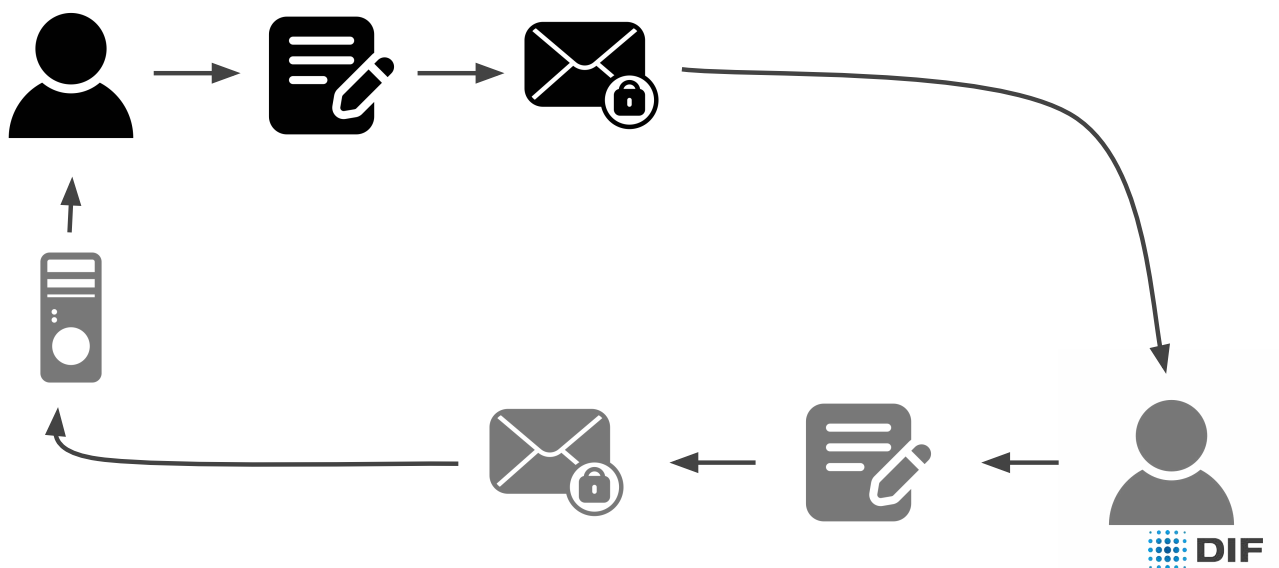
DIDComm is communication
with the subject



DIDComm Message Flow



DIDComm Message Flow



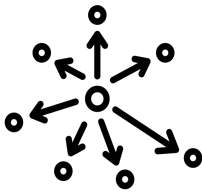
Properties of DIDComm



Secure



Private



Interoperable



Transport-agnostic



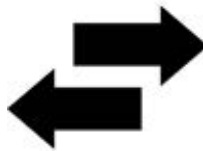
Extensible



Additional Properties of DIDComm



Message-oriented



Asynchronous



Routeable



DIDComm

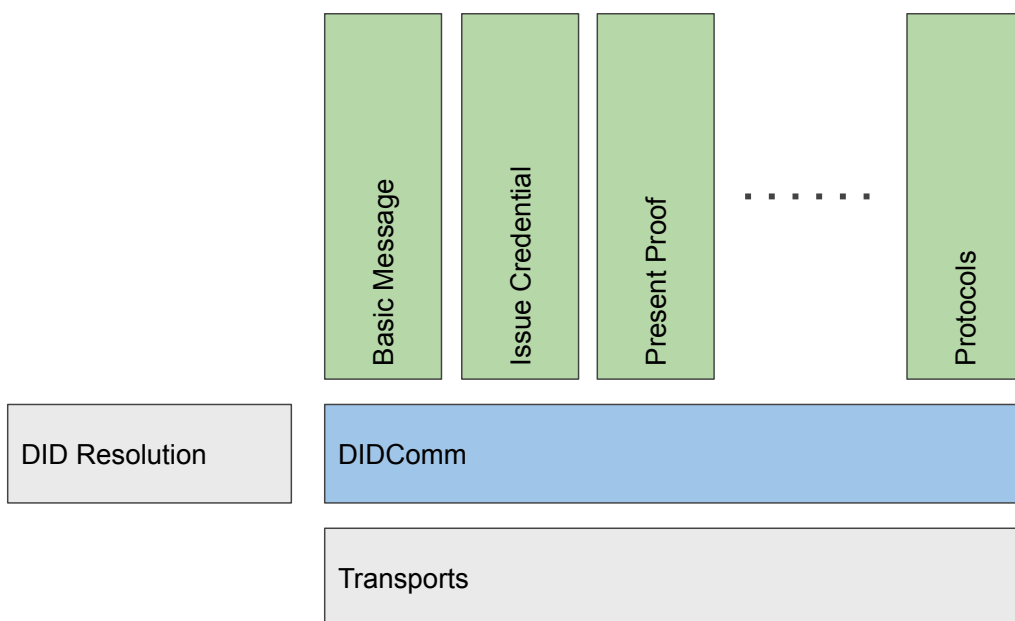
Example Agent Message

```
{  
  "id": "123456780",  
  "type": "https://didcomm.org/basicmessage/2.0/message",  
  "lang": "en",  
  "sent_time": "2022-01-15 18:42:01Z",  
  "body": {  
    "content": "Your hovercraft is full of eels."  
  }  
}
```

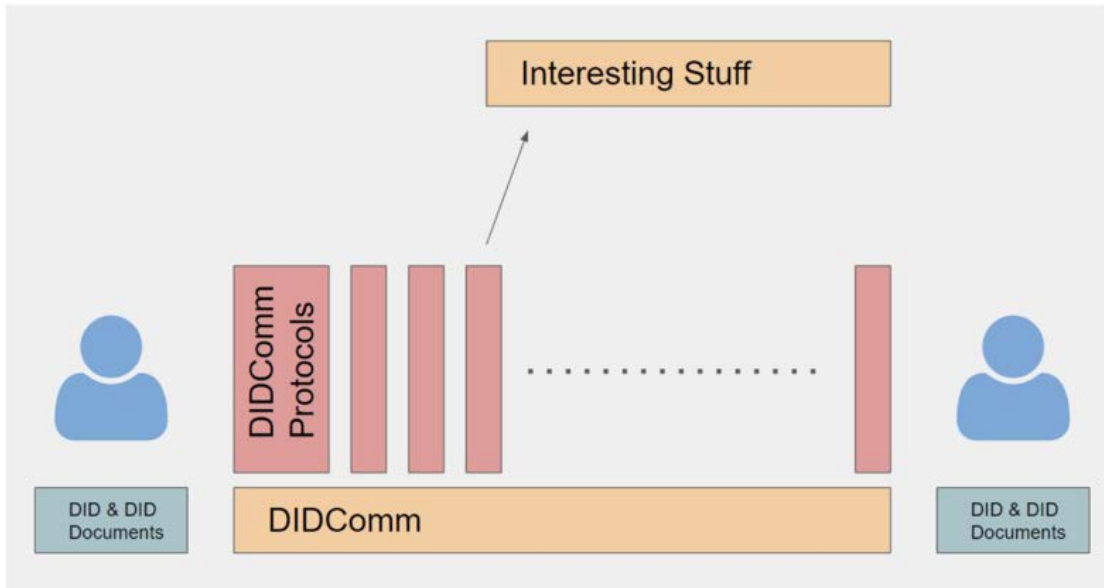
See <https://didcomm.org/basicmessage/2.0/> for details on the protocol



DIDComm



DIDCOMM



<https://www.linkedin.com/pulse/what-didcomm-pictures-indiciotech-hnd0c/>



ConsenSys Mesh Donated Veramo Open-Source Software to DIF



- Create and manage keys for signing and encryption
- Create and manage Decentralized Identifiers (DID)
- Issue Verifiable Credentials (VCs) and Presentations (VPs)
- Verify such VCs and VPs
- Present credentials using Selective Disclosure
- Communicate with other agents using DIDComm (or other protocols)
- Receive, filter, store and serve data
- Control other agents remotely, or act as a proxy for them

Veramo in DIF GitHub repository : <https://github.com/decentralized-identity/veramo>



Thank You

DIF website: <https://identity.foundation>

limari@identity.foundation



Ways You Can Be Involved



- Volunteer as a Developer Advocate + help build hackathons
- Update the draft specification for DWN to match the reference implementation, located [here](#).
- For DID methods, keep the universal drivers up to date with the Universal Resolver
- Create a demo app using DIDcomm or another work item
- Put your hand up to chair a working group
- Run for steering committee

LinkedIn: <https://www.linkedin.com/in/pratapmridha/>

LinkedIn: <https://www.linkedin.com/in/mostafanagy01/>

DIF Volunteer Developer Advocates



Pratap Mridha
Blockchain Core Developer
@Hypermine



Mostafa Nagy
Blockchain / Microservices / DevOps Developer @IBM Digital Credentials



DIF Primary Scope for Digital Identity

DIDs, VCs; Issuer, Holder, Verifier



Decentralized Identifiers (DIDs) v1.0

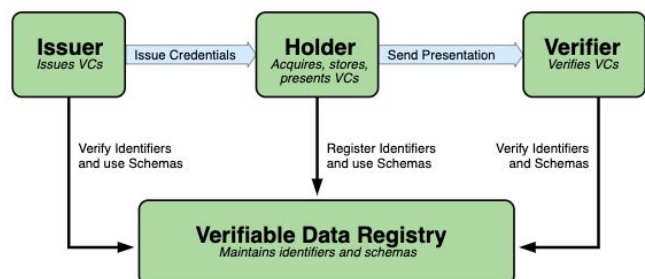
Core architecture, data model, and representations

W3C Recommendation 19 July 2022



Verifiable Credentials Data Model v1.1

W3C Recommendation 03 March 2022

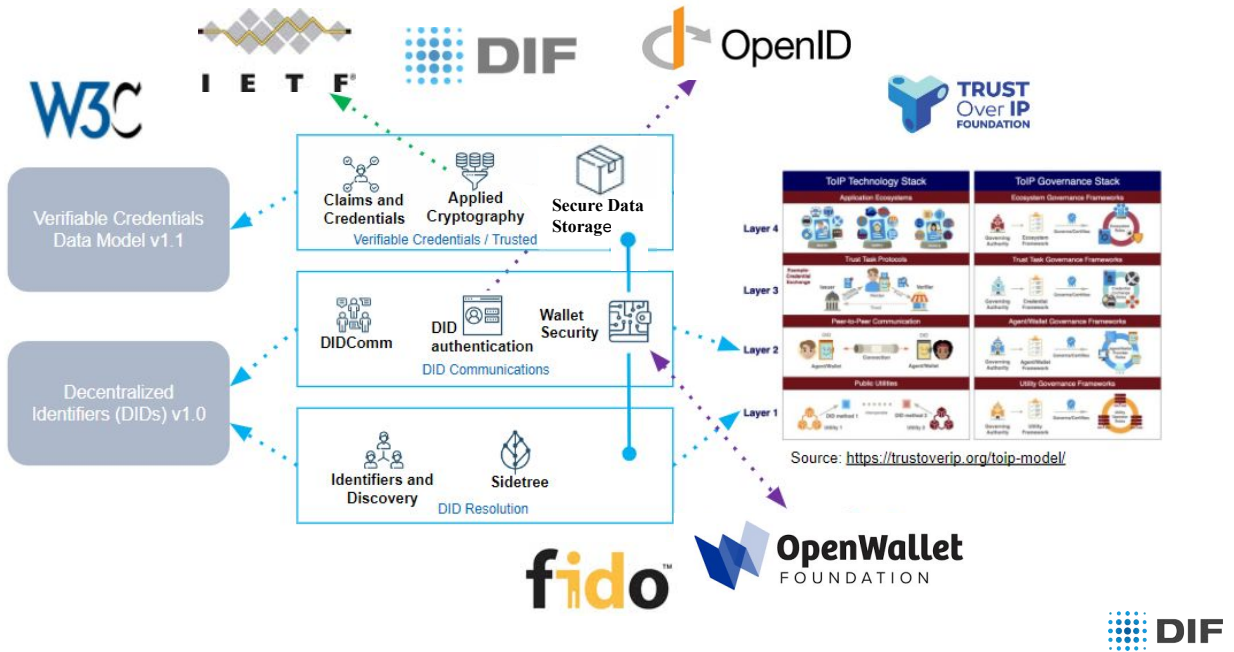


Source: <https://www.w3.org/TR/did-core/>

Source: <https://www.w3.org/TR/vc-data-model/>

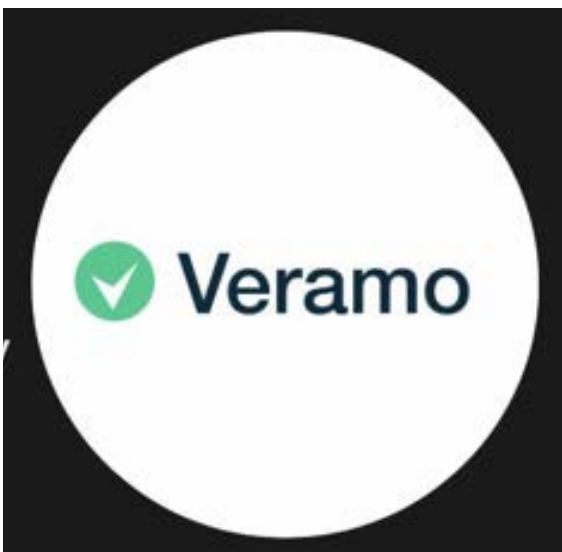


DIF Ecosystem



Source: <https://trustoverip.org/toip-model/>

New Weekly Veramo User Group



If you are looking to become more active in decentralized identity, or open source generally, Veramo is a great way to get started and join this vibrant community. We are looking for help requiring a wide range of expertise:

- Build and/or integrate support for additional standards and protocols, such as Presentation Exchange, SD-JWT, and Aries. In some cases, the implementations exist and just need to be migrated into the Veramo framework.
- Support for new cryptographic key types
- Process/build improvements: helping with formatting and linting commit hooks, developing a test harness for improved test automation

Veramo in DIF GitHub repository : <https://github.com/decentralized-identity/veramo>
<https://veramo.io/>



Decentralized DNS Working Group



Objective: The primary objective of this workgroup is to develop and refine the .zkdid protocol as a decentralised DNS identity protocol based on Zero Knowledge Proofs (ZKPs), incorporating a proof-of-personhood registry for secure and private digital identity management. Emphasis is placed on integrating ZKPs, biometrics, traditional DNS, and decentralised DNS (dDNS), along with robust access control management.



DIF Identifiers and Discovery WG

Charter: "Specifications, implementations, test suites, etc. related to creation, derivation, resolution, management, use of all forms of decentralized identifiers (i.e. including, but not limited to W3C DIDs)"

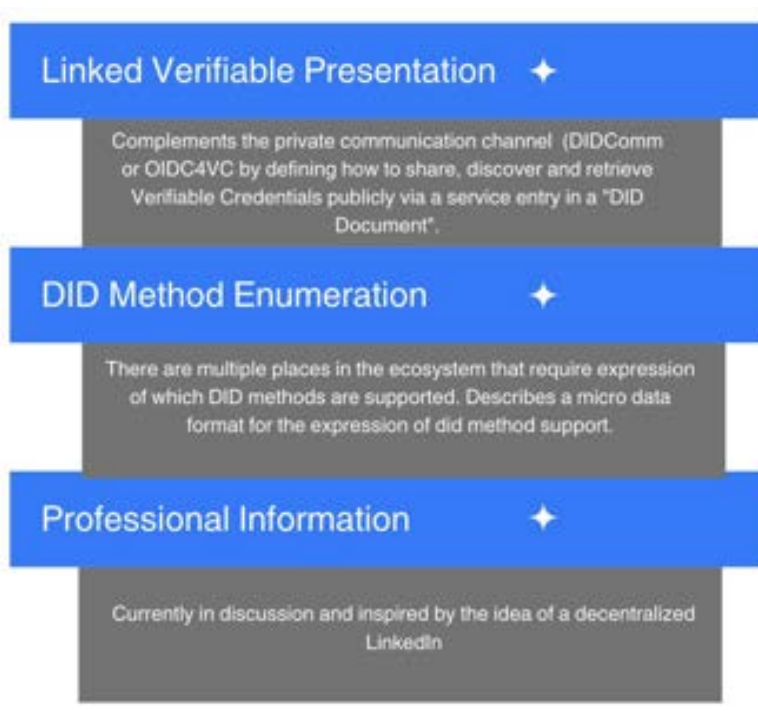
Meetings: Approximately biweekly, since 2019

Some recent topics:

- DID Lint: <https://didlint.ownyourdata.eu/>
- JSON schema for DID documents
- did:btco (Bitcoin Ordinals)
- did:polygonid (Polygon ID)
- DIDs for legal entities and natural persons (GDPR)
- New Universal Resolver/Registrar drivers for did:cheqd, did:ethr, etc.
- DIDs and Nostr

Selected Work Items (Code and Specs)
Universal Resolver
Universal Registrar
did:peer
well-known DID Configuration
JavaScript: did-resolver, ethr-did-resolver, web-did-resolver
TypeScript: did-jwt, did-jwt-vc
Rust did:key library
DID Registration specification
Secret recovery methods
(former) KERI
(former) Sidetree

New DIF Work Items



Source: GitHub,

<https://github.com/decentralized-identity/did-method-enumeration?ref=blog.identity.foundation>

<https://github.com/decentralized-identity/linked-vp>

DIF Activities

DIF Hackathons

- did:hack (June 5-8, 2023)
 - Beginners Hackathon for DID

- DIF Hackathon
 - 422 Registrants
 - 52 Submissions
 - Sponsored Prize pools from TBD, Trinsic, Polygon ID and Ontology



Source:

https://www.linkedin.com/posts/moisesjaramillo_web5-app-wins-didhack-hackathon-activity-7078076016891453440-cZn?utm_source=share&utm_medium=member_desktop

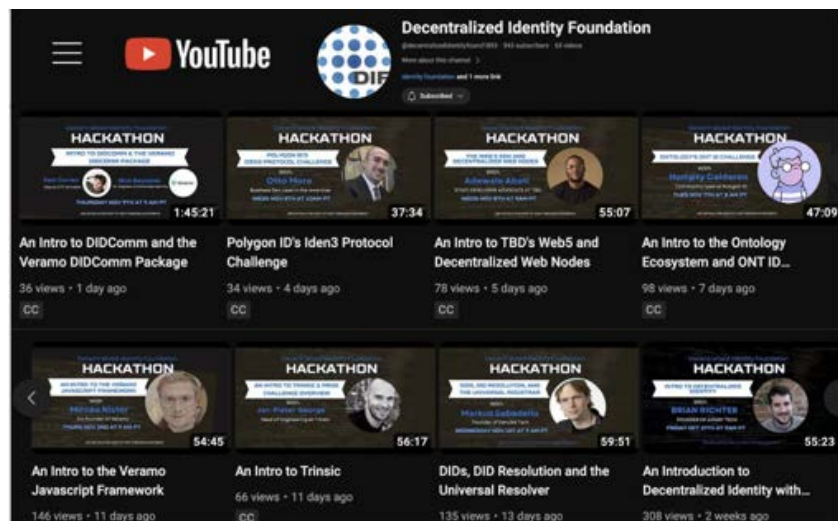
Source: <https://developer.tbd.website/blog/did-hack/>

Source: <https://difhackathon.devpost.com/>



DIF Hackathons

- Playlist with eight educational sessions



Source: <https://youtube.com/playlist?list=PL8i6niRuFWThWi2navqz7MuGNUQpaDASv&feature=shared>



DIF Hackathons

Feedback

- Two of the top three teams were students
- New workgroup on Professional Information from the
- Many used DIDs and VCs for the first time
- DIF Team member was inspired to start a DIF Meetup in India.

Source: <https://x.com/DecentralizedID/status/1745935812087382415?s=20>



DIF Korea SIG



DIF Korea SIG

- Group of experts from industry, academia, and institutions located in Korea for the application of decentralized identity technology
- Focus on activities such as standard technology consultation, opinion collection, policy direction presentation, and core technology demonstration
- Open, non-IPR group, click here to learn more: <https://identity.foundation/SIG-Korea/>

Attendees for DIF Korea SIG Kickoff in July

- Vice President of Korea Information Security Society
- Chairman of the Next Generation Authentication Forum and Member of the Personal Information Protection Committee
- Telecommunications Technology Association (TTA)
- Korea Internet & Security Agency
- Bank of Korea
- Relevant Professors and Researchers
- Blockchain Special Zone Officials
- Many corporate officials

Source: <https://identity.foundation/SIG-Korea/>

Source for DIF Guest blog for Park Kyoung-Chul: <https://blog.identity.foundation/korea-sig/>

Source for DIF newsletter featuring Korea SIG: <https://blog.identity.foundation/dif-newsletter-34/>



Chair for DIF Korea SIG

[Kyoungchul Park](#), CEO K4Security (collaborating with Ministry of Science and Information Communication Technology to research Decentralized Identity)



July kickoff meeting in Busan



Resources to get active

Important Resources

- Get updates on WG Meetings
 - ◆ Slack
 - ◆ Mailing Lists
- Subscribe to the DIF Google Calendar
- Sign the IPR for working groups



Photo by [Ali Kazal](#) on [Unsplash](#)

Mailing Lists: <https://lists.identity.foundation/g/main/subgroups>

For Web Browser: https://calendar.google.com/calendar/embed?src=decentralized.identity%40gmail.com&ctz=America%2FLos_Angeles

iCal format: <https://calendar.google.com/calendar/ical/decentralized.identity%40gmail.com/public/basic.ics>

DIF is a Linux Foundation Project



Part of Linux Foundation

DIF is a Linux Foundation Project, a non-profit 501(c)(6)

IPR Protection

- Specifications created in DIF Working Groups are protected under W3C Patent Policy
- Software is protected under Apache License 2.0

Linux Foundation Digital Trust Initiative

DIF is part of the Linux Foundation “Digital Trust” initiative (May 2023)

Goal:

To improve project discovery and encourage greater collaboration on open source projects with common goals



Source: <https://www.w3.org/Consortium/Patent-Policy/>

Source: <https://www.apache.org/licenses/LICENSE-2.0>

Source: <https://www.linuxfoundation.org/blog/aligning-open-source-projects-with-common-objectives-meet-lf-digital-trust>

Source: <https://www.linuxfoundation.org/projects/digital-trust>



Examples of DIF Contributions, WG Focus

Name	Description	Where Used, Links
Universal Resolver Universal Registrar	Resolve DIDs across different DID methods, based on W3C DID Core 1.0, DID Resolution specifications. Registrar for create, update, deactivate DIDs.	Universal Resolver, https://dev.uniresolver.io/ , DID linter program, https://didlint.ownyourdata.eu/ , DID
Sidetree	A blockchain-agnostic protocol enabling public, permissionless, decentralized DID overlay networks	Used in Identity Overlay Network (ION) , a DID Method implementation using the Sidetree protocol atop Bitcoin
DIDComm	Secure, private, transport-agnostic communication built atop the decentralized design of DIDs. Came from Aries, DIDComm v2.1	Contender for ToIP Trust Spanning Protocol, used by Indicio for Aruba travel, Hyperledger Aries .
Presentation Exchange	A set of data formats Verifiers can use to articulate proof requirements and Holders can use to describe proofs, PE 2.0	Used in OIDC4VC flow, specification is here, https://identity.foundation/presentation-exchange/
Wallet Security	A set of APIs to enable Identity Wallet and Verifier interoperability, Wallet container backup	Coordinating with Open Wallet Foundation (OWF) which does software, DIF does specifications
DID Authentication	Went to OpenID Foundation, became OpenID Connect for VCs (OIDC4VC), also Self-Issued OpenID Provider (SIOP)	OpenID OIDC4VC libraries are here, https://openid.net/sg/openid4vc/libraries/
Decentralized Web Nodes (DWNs)	Data storage and message relay mechanism entities can use to locate public or private permissioned data related to a DID	DWN SDK here, https://github.com/TBD54566975/dwn-sdk-js
Applied Cryptography	BBS signatures was presented to IETF 116 in Yokohama in March, IETF published Draft 03 on July 10, 2023	Used by Trinsic , MATTR , Identity , and others
JSON Web Proof (JWP)	Addition to JOSE family, supports ZKP, includes analog for COSE, a CBOR Web Proof that mirrors the same features	Initial JWP proposal and planned space for the development of this work
Trust Establishment	Specification by which a Party makes trust statements about a given Party for a given Topic using Trust Establishment Documents	Collaborating with Trust over IP (ToIP), implemented by companies such as Cheqd and Indicio


Contents

- **DIF Overview**
 - Scope: DID, VCs; Issuer, Holder, Verifier Model
 - DIF Mission
 - DIF is a Linux Foundation Project
- **DIF Update**
 - DIF Working Groups
 - Examples of DIF Contributions
 - DIF Ecosystem
 - DIF Identifiers and Discovery WG
 - DIF Applied Cryptography (BBS)
 - DIF Hackathon Summary
 - Use Case Example
 - DIF Korea SIG



Why DIF Creates Building Blocks

Vendors build products ...
But ecosystems need building blocks ...



... to make hard things easy
... to ensure they are vibrant and interoperable
... to build-in and not bolt-on privacy and security



Anil John
Technical Director, Silicon Valley Innovation Program
(U.S. Civil Servant)

U.S. Department of Homeland Security



DIF Lifecycle

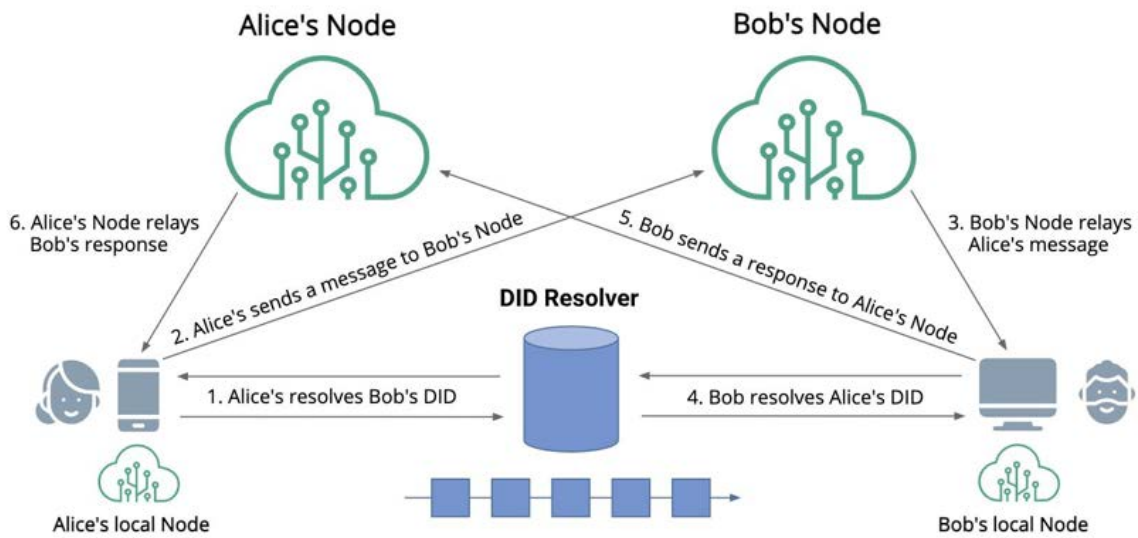


Market Size

Decentralized Identity Market

- \$0.96 Billion in 2022
- \$101.65 Billion by 2030
- CAGR of 88.74% from 2023 to 2030

Decentralized Web Node Topology



Source: <https://identity.foundation/decentralized-web-node/spec/#topology>

Decentralized Digital Identity



Decentralized Identifiers (DIDs) v1.0

Core architecture, data model, and representations

W3C Recommendation 19 July 2022

Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity.

A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID.

Source: <https://www.w3.org/TR/did-core/>

Other Opportunities

- DIF Grants
- On 12 August 2021, The Claims & Credential (C&C) Working Group at DIF gladly announced Transmute Industries as the recipient of the first DIF Grant to provide a JWS Test Suite for Verifiable Credentials.

-

Mailing Lists: <https://lists.identity.foundation/g/main/subgroups>

For Web Browser: https://calendar.google.com/calendar/embed?src=decentralized.identity%40gmail.com&ctz=America%2FLos_Angeles

iCal format: <https://calendar.google.com/calendar/ical/decentralized.identity%40gmail.com/public/basic.ics>



DIDComm

§ Purpose and Scope

The purpose of DIDComm Messaging is to provide a secure, private communication methodology built atop the decentralized design of [DIDs](#).

...

DIDComm Messaging enables higher-order protocols that inherit its security, privacy, decentralization, and transport independence.

Examples include exchanging verifiable credentials, creating and maintaining relationships, buying and selling, scheduling events, negotiating contracts, voting, presenting tickets for travel, applying to employers or schools or banks, arranging healthcare, and playing games.

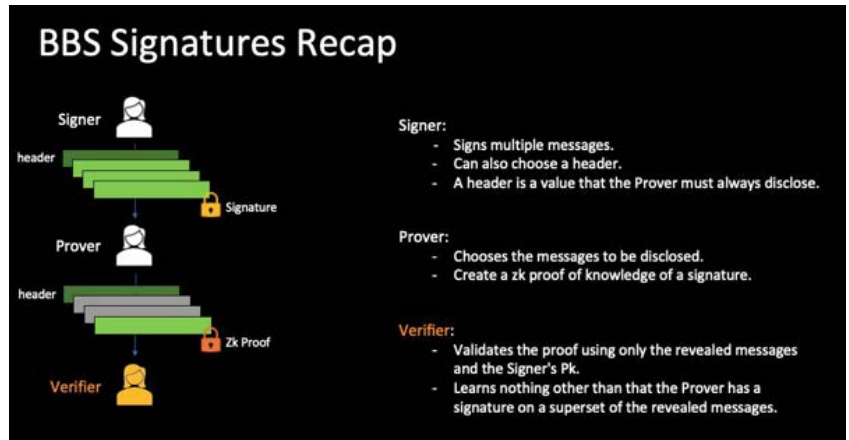
Source: <https://identity.foundation/didcomm-messaging/spec/v2.1/>

BBS Signature Scheme

The BBS Signature Scheme
draft-irtf-cfrg-bbs-signatures-03

Abstract

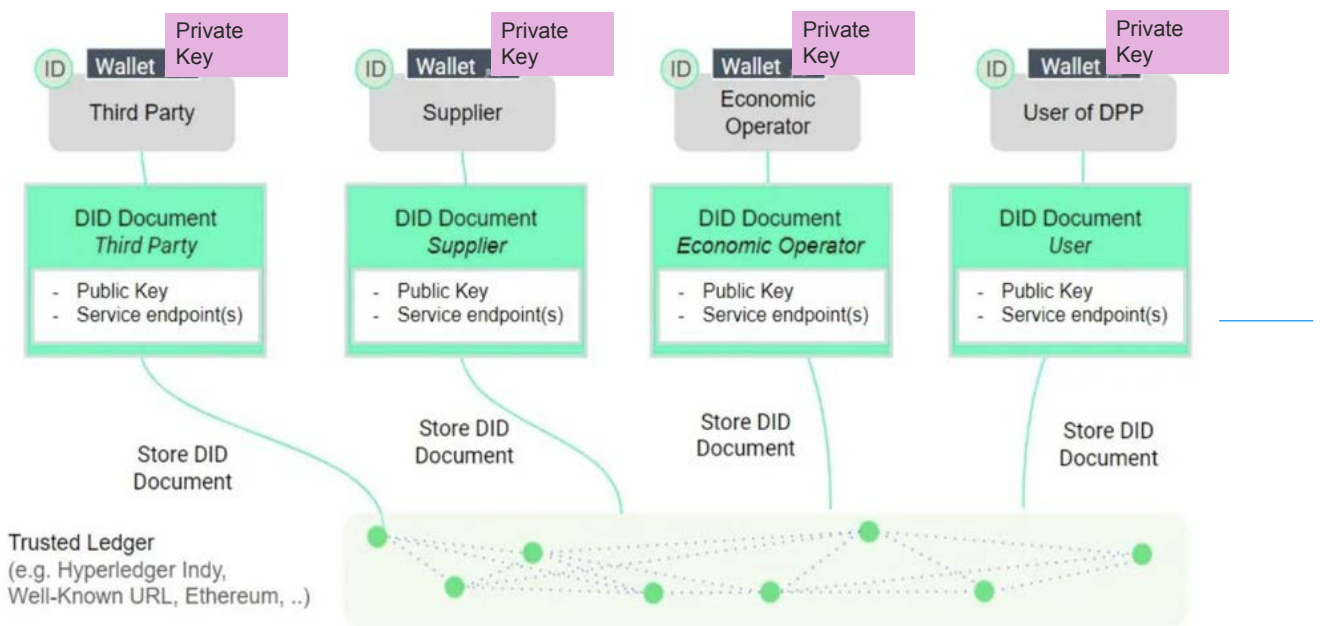
BBS is a digital signature scheme categorized as a form of short group signature that supports several unique properties. Notably, the scheme supports signing multiple messages whilst producing a single output digital signature. Through this capability, the possessor of a signature is able to generate proofs that selectively disclose subsets of the originally signed set of messages, whilst preserving the verifiable authenticity and integrity of the messages. Furthermore, these proofs are said to be zero-knowledge in nature as they do not reveal the underlying signature; instead, what they reveal is a proof of knowledge of the undisclosed signature.



Source: <https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/03/>

Source: BBS deck, <https://datatracker.ietf.org/meeting/116/proceedings/>, click on *The BBS Signature Scheme*

Example Use Case: EU Digital Product Passport (DPP)

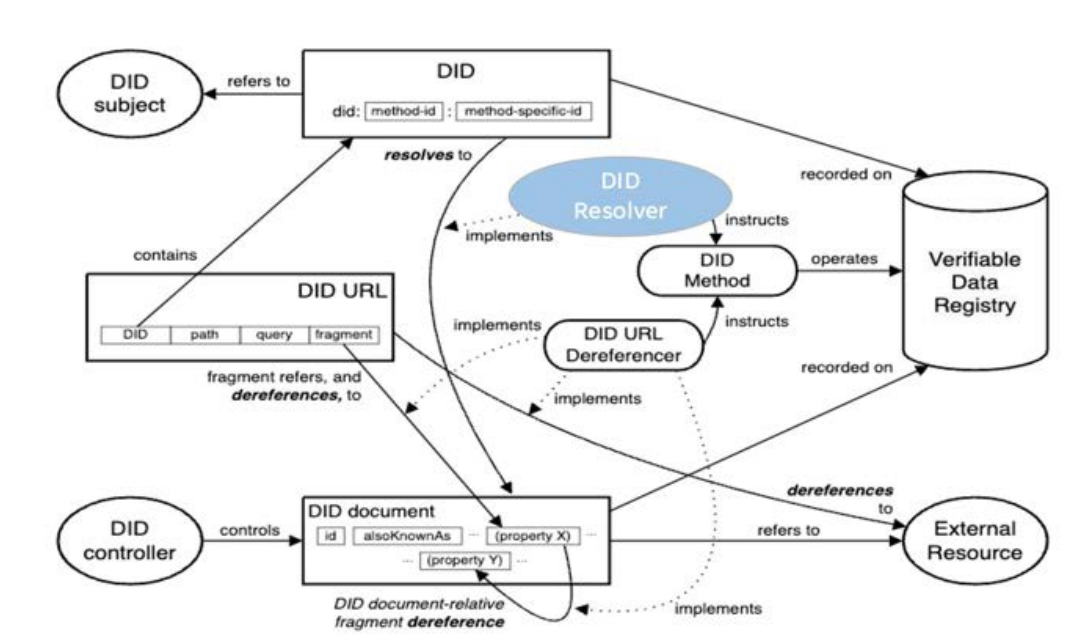


Source: <https://medium.com/@susi.guth/implementing-digital-product-passports-using-decentralized-identity-standards-f1102c452020>

Backup Slides



DID Resolver



DIF collaborates with our Liaison Partners to build the ecosystem



Decentralized Identity Myths

Myths

- W3C Recommendations define DIDs and VCs
- Our work is done

Reality

- We are just beginning



Events at ETHDenver (March 2023)

- WalletCon
- ETHDenver Climate Summit, panel, *How Decentralized Identity Will Change the Climate Accountability Conversation*
- did:day – Half-day event focused on DIDs

DID = Decentralized Identifier
VC = Verifiable Credential
W3C = World Wide Web Consortium

76

Why decentralized identity?

Decentralized identity enables **control** over data and brings **trust** to digital interactions.

It enables numerous **commercial use cases** beyond identity verification and authentication.

Self-Sovereign Identity has been adopted as a **policy goal** by legislatures including Canada, Bhutan and EU



<https://www.gartner.com/reviews/market/decentralized-identity-solutions>
<https://www.wipro.com/innovation/improve-detection-of-online-frauds-using-decentralized-identity-management/#>
https://www.europarl.europa.eu/doceo/document/ITRE-PR-732707_EN.pdf



References

- Allen, Christopher; Brock, Arthur; Buter, Vitalik; Callas, Jon; Dorje, Duke; Lundkvist, Christian; Kravchenko, Pavel; Nelson, Jude; Reed, Drummond; Sabadello, Markus; Slepak, Greg; Thorp, Noah; Wood, Harlan T. *Decentralized Public Key Infrastructure* (December 2015), <https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/dpki.pdf>
- Askin, Jonathan; Foucek, Chynna; Abualy, Sydney; Furs, Alexei. *Trust in a Trustless System: Decentralized, Digital Identity, Customer Protection, and Global Financial Security* (January 2022), <https://law.mit.edu/pub/trustinatrustlesssystem/release/1>
- Baya, Vinod. *Digital Identity, Moving to a Decentralized Future*, (October 2019), <https://www.citi.com/ventures/perspectives/opinion/digital-identity.html>
- Bicacki, Kemal; Crispo, Bruno; Tanenbaum, Andrew. *How to Incorporate Revocation Status Information into the Trust Metrics for Public-Key Certification* (March 2005), <https://dl.acm.org/doi/pdf/10.1145/1066677.1067037> (Requires ACM Membership)
- Boneh, Fan. *DeFi Lecture 11: Decentralized Identity* (November 2021), <https://www.youtube.com/watch?v=3FL-1HMKvYA>
- Chang, Wayne. *Upgradeable Decentralized Identity – DID Method Traits* (July 2022), <https://blog.spruceid.com/upgradeable-decentralized-identity/>
- Chang, Wayne. *Sign-in with Ethereum* (January 2023), https://www.youtube.com/watch?v=VHwzE6mVm_s
- Collins, Benjamin. *Beyond Blockchain: How Decentralized Identifiers Work* (February 2023), <https://medium.com/transmute-techtalk/beyond-blockchain-how-decentralized-identifiers-dids-work-20bb199d038>
- Cooper, David A., Computer Security Division, NIST, *A Closer Look at Revocation and Key Compromise in Public Key Infrastructures*, <https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/paper2.pdf>
- DIDComm V2 Guidebook (2022), <https://didcomm.org/book/v2/didrotation>
- DID the Decentralized Identifier, <https://decentralized-id.com/web-standards/w3c/wg/did/decentralized-identifier/>
- Fdhila, Walid; Stifter, Nicholas; Kostal, Kristian; Saglam, Cihan; Sabadello, Markus. *Methods for Decentralized Identities: Evaluation and Insights*, <http://eprints.cs.univie.ac.at/7094/1/2021-1087.pdf>



References

- Fernandes, Bruno Miguel Gomes. Self-Sovereign Identity Decentralized Identifiers, Claims and Credentials using non Decentralized Ledger Technology (November 2021), https://repositorium.sdum.uminho.pt/bitstream/1822/82791/1/Bruno%20Miguel%20Gomes%20Fernandes.pdf?utm_source=substack&utm_medium=email
- Genise, Nick; Balenson T., David. *Cryptography Review of W3C Verifiable Credentials Data Model (VCDM) and Decentralized Identifiers (DIDs) Standards and Cryptography Implementation Recommendations* (October 2021), <http://www.csl.sri.com/papers/vcdm-did-crypto-recs/crypto-review-and-recs-for-VCDM-and-DIDs-implements-FINAL-20211015.pdf>
- Guth-Orlowski, Susanne; Ebert, Johannes; Thiermann, Ricky. *Implementing Digital Product Passports using decentralized identity standards* (April 2023), <https://medium.com/@susi.guth/implementing-digital-product-passports-using-decentralized-identity-standards-f1102c452020>
- Jacques, Samuel; Lodder, Michael; Montgomery, Hart. *ALLOSAUR: Accumulator with Low-Latency Oblivious Sublinear Anonymous credential Updates with Revocations* (October 2022), <https://eprint.iacr.org/2022/1362.pdf>
- Brunner, Clemens; Gellersdörfer, Ulrich; Knirsch, Fabian; Engel, Dominik; Matthes, Florian. *DID and VC: Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust* (December 2020), <https://dl.acm.org/doi/fullHtml/10.1145/3446983.3446992>
- MATTR, *Create a Static Key DID*, <https://learn.mattr.global/tutorials/dids/did-key>
- Park Chang-Seop; Nam, Hye-Min. *A New Approach to Constructing Decentralized Identifier for Secure and Flexible Key Rotation* (October 2021), <https://ieeexplore.ieee.org/abstract/document/9583584>
- Pope, Nick; Tabor, Michał; Barreira, Iñigo; Nicholas Dunha; Granc, Franziska; Thiell, Christoph; Fiedler, Arno (ENISA). *Digital Identity: Leveraging the SSI Concept to Build Trust* (January 2022), <https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust>
- Thorstensson, Joel. *Key Revocation in Self-Certifying Protocols* (April 2022), <https://blog.ceramic.network/key-revocation-in-self-certifying-protocols/#:~:text=Key%20revocation%20%2D%20a%20function%20in,the%20new%20key%20becomes%20active>

References

- Rocco, Gregory. *Decentralized Identity and Web3* (August 2022), <https://blog.spruceid.com/decentralized-identity-and-web3/>
- Sabadello, Markus. *The Power of DIDs #2: Creating DIDs* (April 2023), https://www.linkedin.com/posts/danube-tech_the-power-of-dids-2-creating-dids-activity-7051844692723789824-2UjD?utm_source=share&utm_medium=member_desktop
- Smith, Samuel. *Key Event Receipt Infrastructure (KERI): A secure identifier overlay for the internet* (May 2020), <https://www.youtube.com/watch?v=izNZ20XSXR0>
- Sporny, Manu. *Verifiable Credentials and DIDs* (September 2022), <https://www.youtube.com/watch?v=Nk8Ey0MC528>
- W3C Recommendation, *Decentralized Identifiers (DIDs) v1.0. Core architecture, data model, and representations* (July 2022), <https://www.w3.org/TR/did-core/>
- Weston, Georgia. *Self Sovereign Identity & Decentralized Identity – An Unlimited Guide* (July 2022), <https://101blockchains.com/self-sovereign-identity-and-decentralized-identity/>
- Windley, Philip. *Digital Identity Design, Deploy, and Manage Identity Architectures* (February 2023), O'Reilly Media

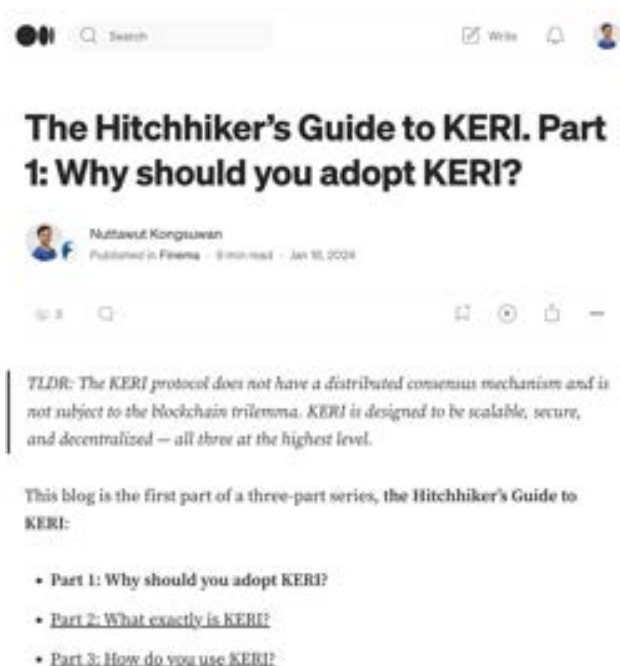
The Hitchhiker's Guide to KERI

IIWXXXVIII: April 16, 2024

Nuttawut Kongsuwan, Finema



<http://bit.ly/keri-iiw38>



<http://bit.ly/keri-iiw38>

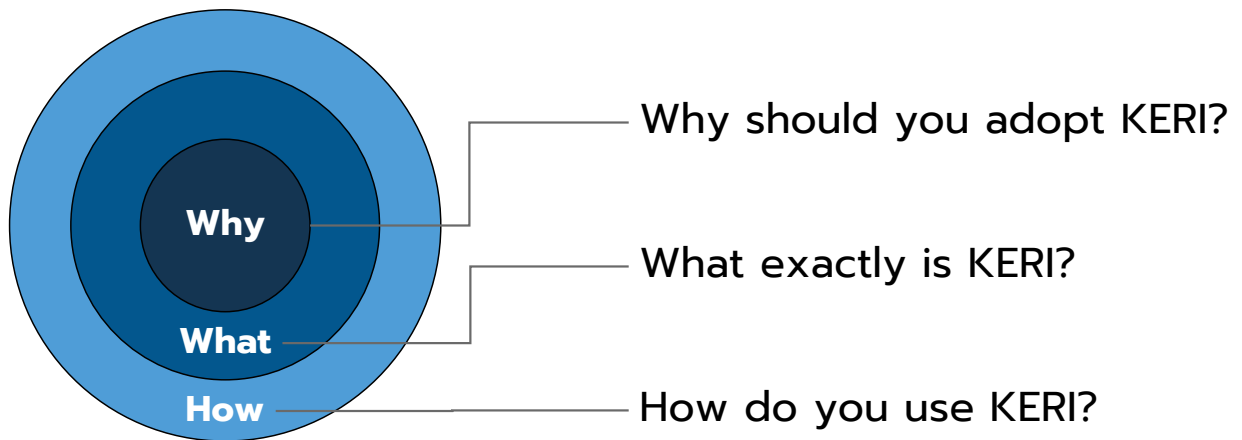
Medium Blog Posts

Part 1: Why
<https://medium.com/finema/the-hitchhikers-guide-to-keri-part-1-51371f655bba>

Part 2: What
<https://medium.com/finema/the-hitchhikers-guide-to-keri-part-2-what-exactly-is-keri-e46a649ac54c>

Part 3: How
<https://medium.com/finema/the-hitchhikers-guide-to-keri-part-3-how-do-you-use-keri-2d1724afa432>

KERI Why / What / How



Adapted from "The Golden Circle" by Simon Sinek

3

KERI Why

4

**Centralized
Digital Identity**
(1970s)

**Blockchain-based
Decentralized
Digital Identity**
(2015)

**KERI-based
Decentralized
Digital Identity**
(2019)

5

Cryptocurrency System

Alice $\xrightarrow{2 \text{ btc}}$ Bob

If Alice transfers 2 btc twice, she is twice as poor.

Double-Spending Proof is necessary.

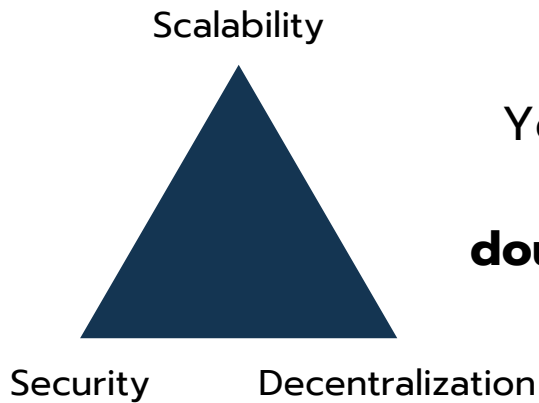
Identity System

Alice $\xrightarrow{\text{authorizes}}$ Bob

If Alice authorizes Bob twice, nothing changes the second time.

Double-Spending Proof is unnecessary.

Blockchain Trilemma



You can get all three
by giving up
double-spending proof.

7

KERI Why

1. KERI is a more **scalable** alternative to blockchain for building **decentralized identity** systems.
2. KERI is portable with or without blockchains.
3. KERI is recoverable from Quantum Attack.

8

KERI What

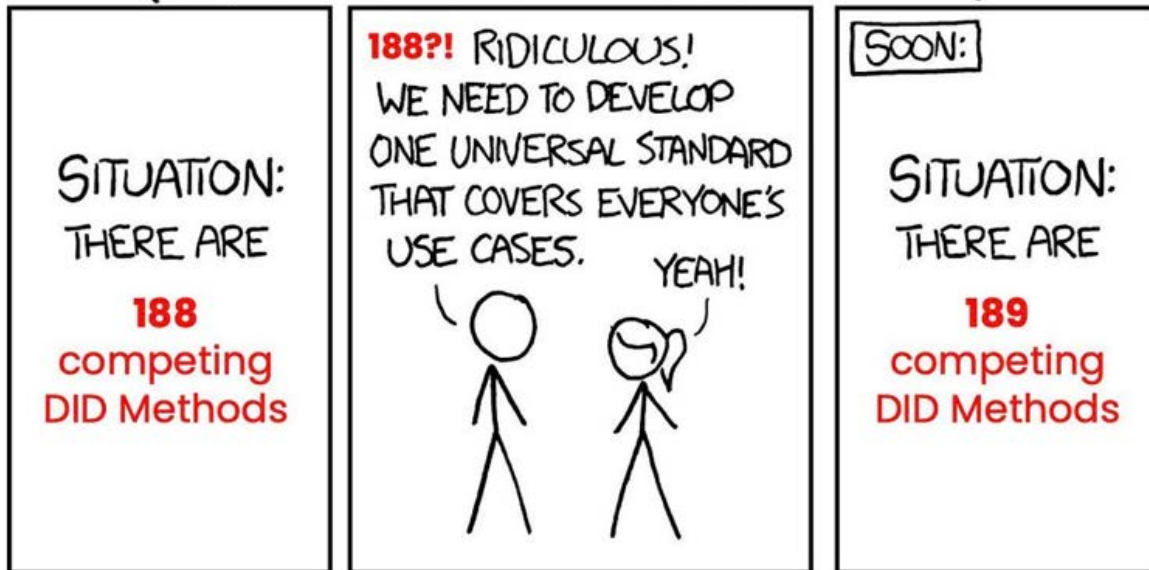
9

<http://bit.ly/keri-iiw38>

1. KERI is a DID Method

10

HOW DID Methods PROLIFERATE: (SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)



Unofficial Draft

TABLE OF CONTENTS

- Abstract
- Status of This Document
- 1. Introduction
- 2. Concepts
 - 2.1 Events
 - 2.2 Key Event Log
 - 2.3 Key Event Receipt Log
 - 2.4 Key State
 - 2.5 Resolver Metadata
 - 2.6 The DID Document
- 3. The did:keri Format
 - 3.1 Method Name
 - 3.2 Method Specific Identifier
- 4. Operations
 - 4.1 Create
 - 4.2 Read
 - 4.3 Update
 - 4.4 Deactivate

The did:keri Method v0.1

A DID Method for KERI Identifiers

Unofficial Draft 10 November 2021

▼ More details about this document

Latest published version:
<https://www.w3.org/keri/>

Latest editor's draft:
<https://decentralized-identity.github.io/keri/>

History:
[Commit history](#)

Editor:
Dr. Sam Smith (ProSapien)


Authors:
[Dr. Sam Smith \(ProSapien\)](#)
[Charles Cunningham \(Jolocom, Spruce\)](#)
[Phil Fearheller \(Scoir, Inc.\)](#)

Feedback:
[GitHub decentralized-identity/keri](#) (pull requests, new issue, open issues)

Copyright © 2021 the document editors/authors. Text is available under the [Creative Commons Attribution 4.0 International Public License](#); additional terms may apply.

1 1 ReSpec

UNOFFICIAL

Table of Contents  Issues (12)

1. Abstract
2. Status of This Memo
3. Copyright Notice
4. Introduction
5. Requirements, Notation and Conventions
 5.1 Keywords
 5.2 Conventions
6. Core Characteristics
 6.1 Method Name
 6.2 Method-Specific Identifier
 6.3 Target System(s)
 6.4 AID controlled identifiers
 6.5 Handling Web Redirection
 6.6 DID Method Operations
 6.6.1 Create
 6.6.2 Read (Resolve)
 6.6.3 Update
 6.6.4 Deactivate
7. DID Documents
 7.1 DID Subject
 7.2 DID Controller

ToIP **did:webs** Method Specification v0.9.15

Specification Status: Implementors Draft

In order to further validate and improve the specification and to demonstrate interoperability between multiple implementations of did:webs, we encourage additional did:webs implementations to the original [did:webs Reference Implementation](#).

Latest Draft:
<https://github.com/trustoverip/tswg-did-method-webs-specification>

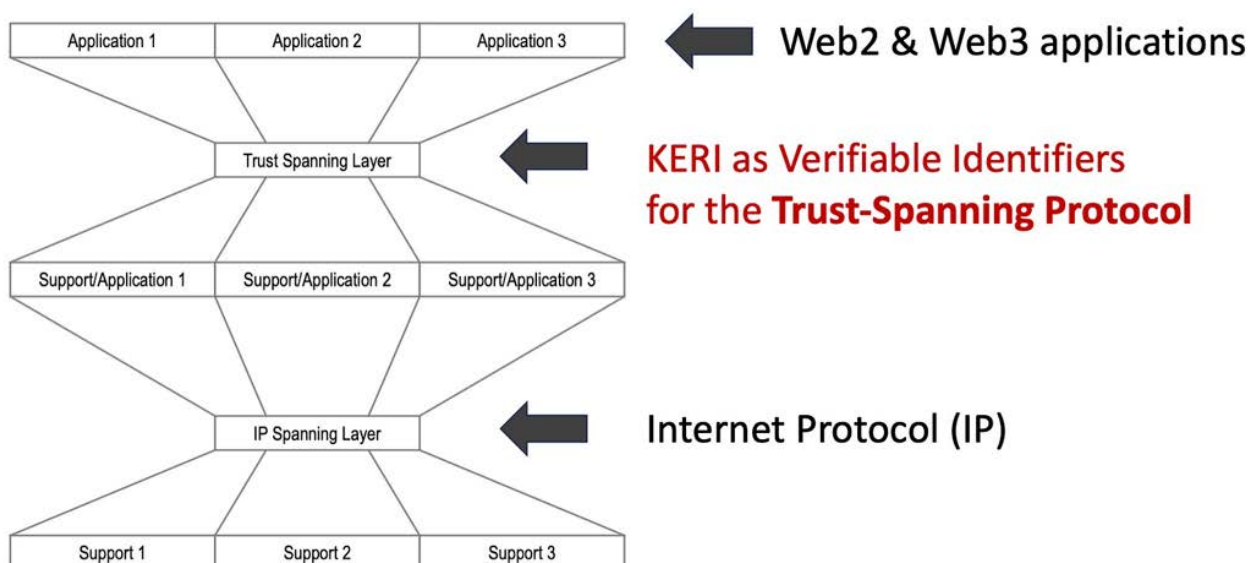
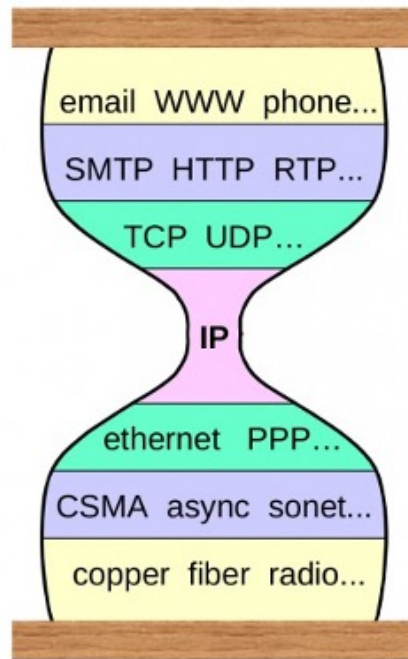
Editors:

- [Phil Feairheller, GLEIF](#)
- [Daniel Hardman, Provenant, Inc](#)
- [Sam Smith, Prosaplen](#)
- [Lance Byrd, GLEIF](#) and [RootsID](#)

Contributors:

- [Markus Sabadello, Danube Tech](#) and [DIF](#)
- [John Jordan, Government of British Columbia](#) and [Trust Over IP Foundation](#)
- [Kevin Griffin, GLEIF](#)
- [Charles Lanahan](#)
- [Nuttawut Kongsuwan, Finema](#)
- [Darrell O'Donnell, Continuum Loop, Inc.](#)

2. KERI is an Identity Overlay of the Internet

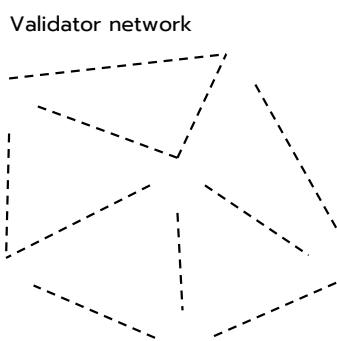


3. KERI is a blockchain without distributed consensus (i.e., microledger)

17

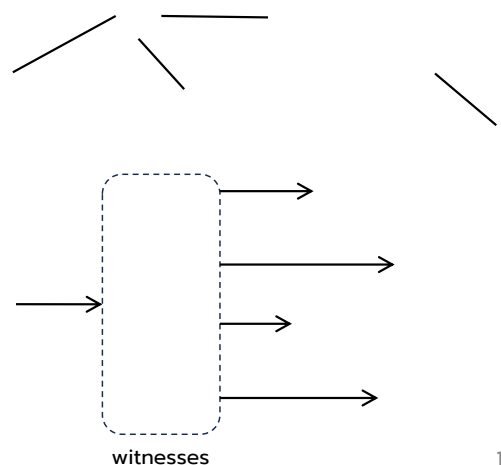
Blockchain

- Distributed consensus ledger
- Total ordering of transactions
- Shared governance



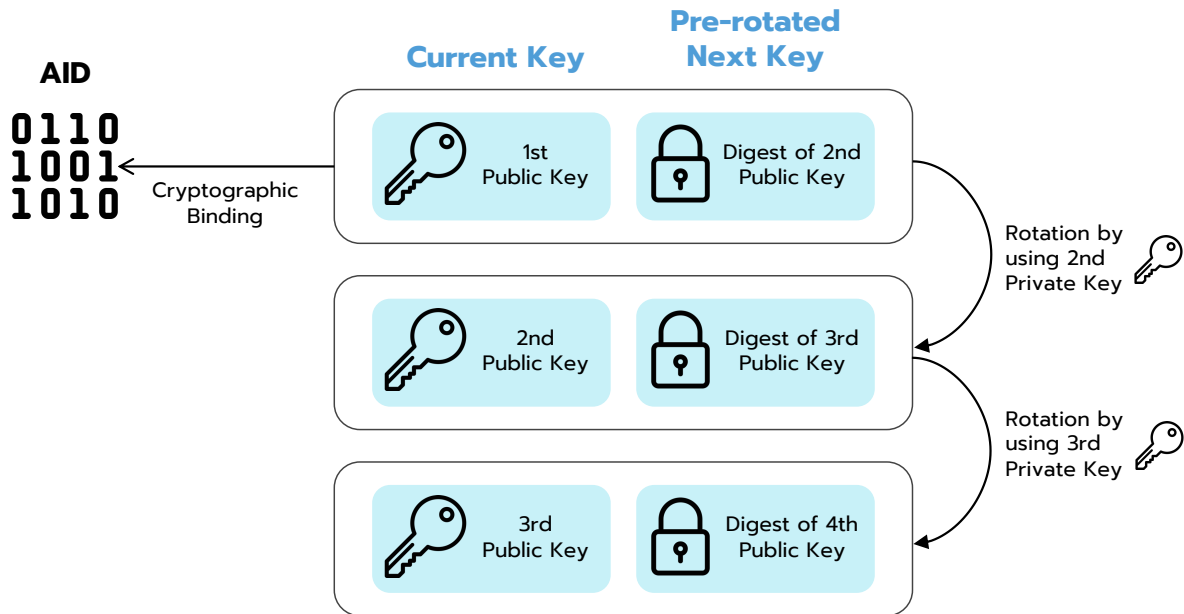
KERI

- A variant of a blockchain without shared distributed consensus
- **Shared data without shared governance**

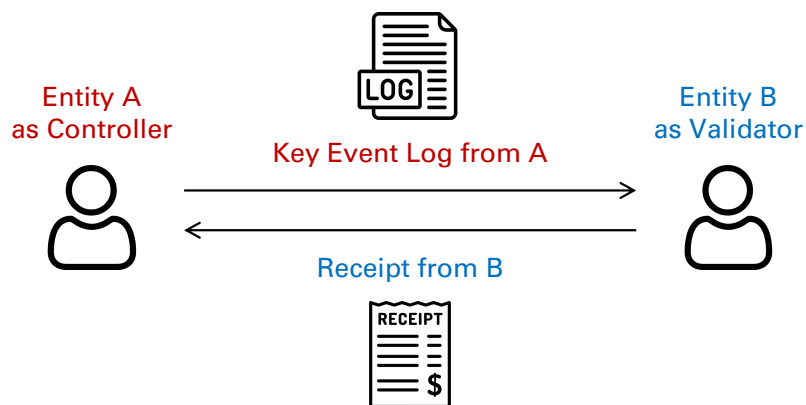


18

Pre-Rotation

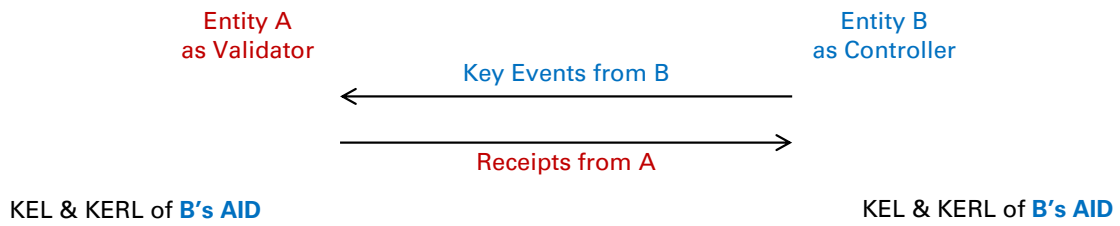
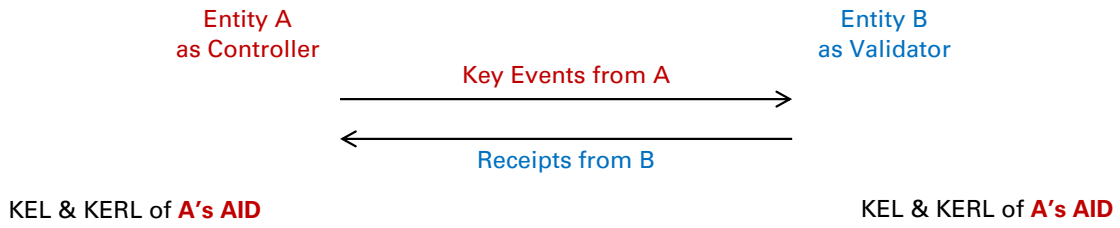


Key Event Receipt



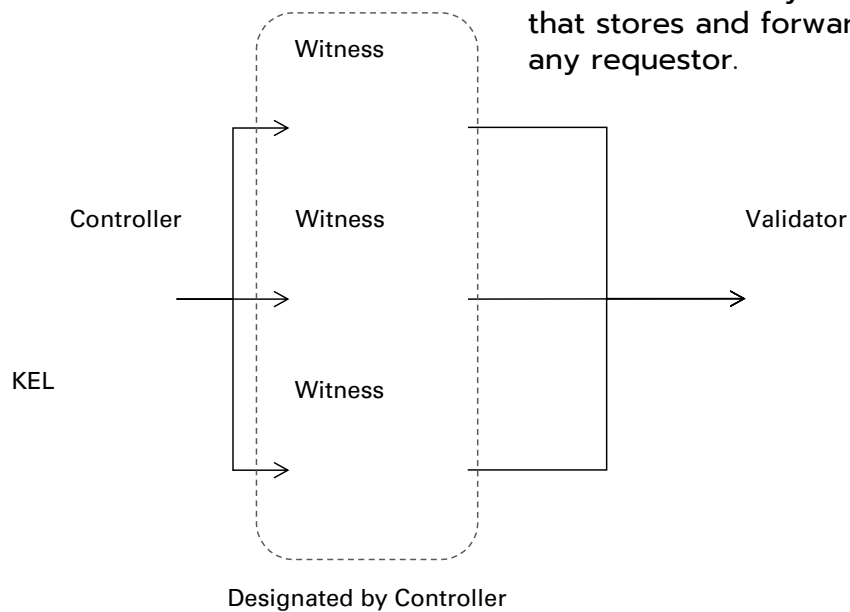
- A KEL may be exchanged directly.
- A key event receipt with a signature is sent back as an acknowledgment.

Peer-to-peer Exchanges



Key Event Witnesses

- A controller may not always be online.
- The controller may designate witnesses that stores and forward key events to any requestor.



KERI in a nutshell

- **Key** – asymmetric key cryptography.
- **Event** – a series of key events related to the management of Autonomic Identifiers (AIDs) using pre-rotation.
- **Receipt** – signed receipts from validators or witnesses of key events
- **Infrastructure** – an open-source framework and protocol for building decentralized identity systems.



KERI How

The KERI Whitepaper (July, 2019)

KEY EVENT RECEIPT INFRASTRUCTURE (KERI) DESIGN ¹²

Samuel M. Smith Ph.D.

v2.60 2021/05/07, original 2019/07/03

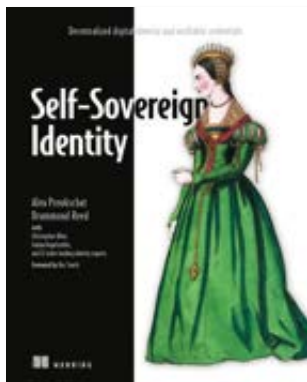
Abstract—An identity system based secure overlay for the Internet is presented. This includes a primary root-of-trust in self-certifying identifiers. It presents a formalism for Autonomic Identifiers (AIDs) and Autonomic Namespaces (ANs). They are part of an Autonomic Identity System (AIS). This system uses the design principle of minimally sufficient means to provide a candidate trust spanning layer for the internet. Associated with this system is a decentralized key management infrastructure (DKMI). The primary root-of-trust are self-certifying identifiers that are strongly bound at issuance to a cryptographic signing (public, private) key-pair. These are self-contained until/unless control needs to be transferred to a new key-pair. In that event an append only chained key-event log of signed transfer statements provides end verifiable control provenance. This makes intervening operational infrastructure replaceable because the event logs may be served up by any infrastructure including ambient infrastructure. End verifiable logs on ambient infrastructure enables ambient verifiability (verifiable by anyone, anywhere, at anytime).

27

Introductory Contents

Textbook

Alex Preukschat & Drummond Reed, "Self-Sovereign Identity", Manning Publication (2021) — Section 10.8



Tutorials & Demos

- [KERI Tutorial Series \(1\)](#), by Kent Bull
- [KERI Tutorial Series \(2\)](#), by Kent Bull
- [KERI & OOB CLI Demo](#), by Phillip Fairheller & Henk van Cann

Blogs & Presentations:

- [KERI for Muggles](#), by Drummond Reed & Sam Smith
- [SSI Meetup KERI Presentation](#), by Sam Smith
- [The Architecture of Identity Systems](#), by Phil Windley
- [KERI jargon in a nutshell](#), by Nuttawut Kongsuwan

KERI Search Engine & Wiki:

- [KERISSE](#), by Henk van Cann and Kor Dwarshuis

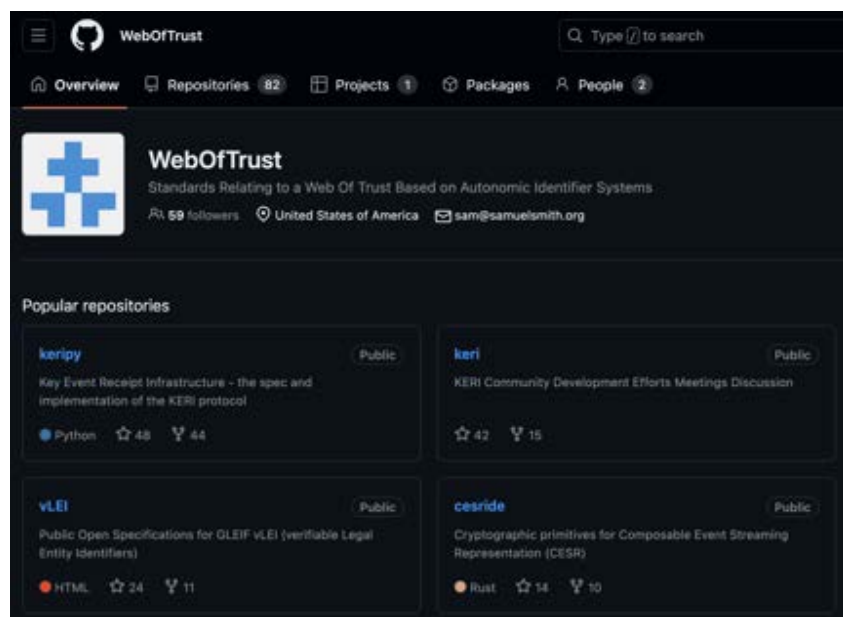
28

KERI and Related Specifications

- **[Key Event Receipt Infrastructure \(KERI\)](#)**: the specification for the KERI protocol itself.
- **[Authentic Chained Data Containers \(ACDC\)](#)**: the specification for the variant of Verifiable Credentials (VCs) used within the KERI ecosystem.
- **[Composable Event Streaming Representation \(CESR\)](#)**: the specification for a dual text-binary encoding format used for messages exchanged within the KERI protocol.
- **[DID Webs Method Specification](#)**: the specification did:webs method that improves the security property of did:web with the KERI protocol.

29

KERI Open-Source Projects



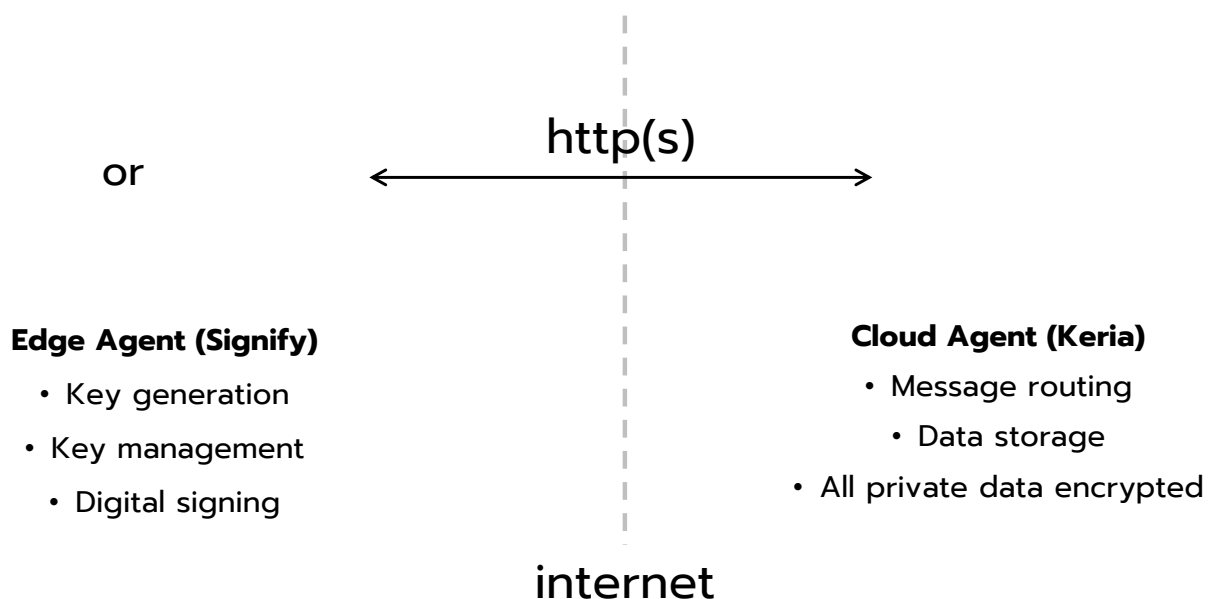
30

Important Projects

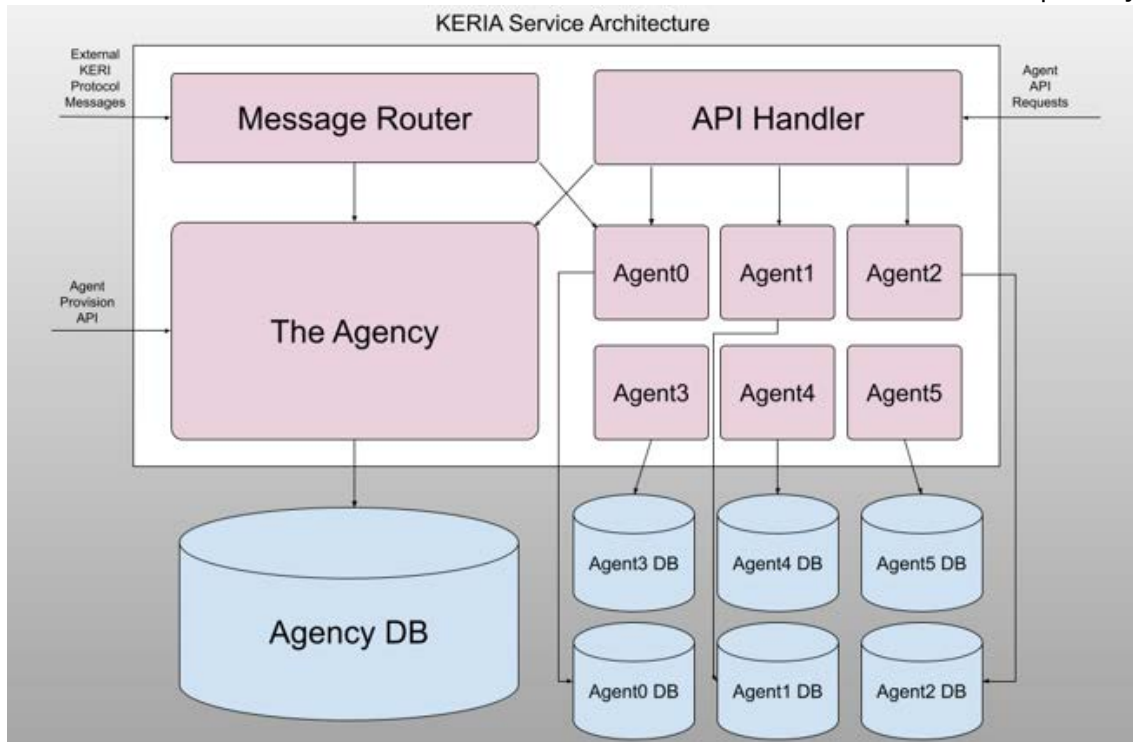
- Reference Implementation
 - KERIpy (Python) <https://github.com/WebOfTrust/keripy>
- Edge Agent: Signify
 - SignifyPy (Python) <https://github.com/WebOfTrust/signifypy>
 - Signify-TS (Typescript) <https://github.com/WebOfTrust/signify-ts>
- Cloud Agent: KERIA
 - KERIA (Python): <https://github.com/WebOfTrust/keria>

31

Key-At-The-Edge (KATE) Protocol



32



KERI Command Line Interface (KLI)

KERI Command Line Interface (KLI)

```
usage: kli [command] [subcommand] ...
```

KLI is a command line tool to perform basic KERI operations, including:

- Identifier (AID) creation
- Key management (inception and rotation)
- KEL query
- Participation in delegated identifiers
- Participation in multi-signature group identifiers.
- Signing and verifying
- Issuance of credentials (ACDCs)
- Running witnesses
- Running watchers

35

KERIPy Installation

```
# Step 1: Install Python 3.10.4+

# Step 2: Install libsodium 1.0.18
# Download a tarball from https://download.libsodium.org/libsodium/releases/
# cd to decompressed tarball's directory
./configure
make && make check
sudo make install

# Step 3: Install KERIPy
git clone https://github.com/WebOfTrust/keripy.git
pip install -r requirements.txt

# Step 4: Check if KLI works
kli version
```

For a more detailed installation guide, I recommend a tutorial by Kent Bull.
<https://kentbull.com/2023/03/09/keri-tutorial-series-treasure-hunting-in-abydos-issuing-and-verifying-a-credential-acdc/>

36

Running KLI Demo Script

Reference: <https://github.com/WebOfTrust/keripy/blob/development/scripts/demo/basic/demo-script.sh>

```
# First, cd to keripy's root directory
# Then, cd to its demo directory
cd scripts/demo/

# Set up environment variables
# KERI_DEMO_SCRIPT_DIR = {keripy_root_dir}/scripts/demo
# KERI_SCRIPT_DIR = {keripy_root_dir}/scripts/
# KERI_TEMP_DIR = scripts_tmp
source demo-scripts.sh

# Run the demo script
./basic/demo-scripts.sh
```

```
+ Workspace cd keripy
+ keripy git:(development) cd scripts/demo
+ demo git:(development) source demo-scripts.sh
+ demo git:(development) ./basic/demo-script.sh
KERI Keystore created at: /Users/nkongsuwan/.keri/ks/scripts_tmp/test
KERI Database created at: /Users/nkongsuwan/.keri/db/scripts_tmp/test
KERI Credential Store created at: /Users/nkongsuwan/.keri/reg/scripts_tmp/test
Prefix: BIGaILyWpZbVXbQcZcIARX1jW0nmJ76no15rMtc
Public key 1: BIGaILyWpZbVXbQcZcIARX1jW0nmJ76no15rMtc

ERR: Attempt to rotate nontransferable pre=BIGaILyWpZbVXbQcZcIARX1jW0nmJ76no15rMtc.
Prefix: EIryzWYLZ9bQr7EHMAo8Xk4r2h-OgaEqERid7-AWp6o
Public key 1: DKLZ887vfaKLr82SLfEcKH11QwCacR5nZKiesQhWe

Prefix: EIryzWYLZ9bQr7EHMAo8Xk4r2h-OgaEqERid7-AWp6o
New Sequence No. 1
Public key 1: DAZJzOSC3bcEC1ZFgy_uMzeaxSVLSTYdXZo7hueDzr
Prefix: EIryzWYLZ9bQr7EHMAo8Xk4r2h-OgaEqERid7-AWp6o
New Sequence No. 2
Public key 1: 2HZae85WY6okbuARIPhow6vIof9_1FARE1rG-ver69H
Prefix: EIryzWYLZ9bQr7EHMAo8Xk4r2h-OgaEqERid7-AWp6o
New Sequence No. 3
Public key 1: 2HZae85WY6okbuARIPhow6vIof9_1FARE1rG-ver69H
Prefix: EIryzWYLZ9bQr7EHMAo8Xk4r2h-OgaEqERid7-AWp6o
New Sequence No. 4
Public key 1: DP85WbTHqKQGb8LbV5QDJE-NojvMAv-5uW3Xby4zf
Prefix: EIryzWYLZ9bQr7EHMAo8Xk4r2h-OgaEqERid7-AWp6o
New Sequence No. 5
Public key 1: DB19KtMyWcESJxVMU0tpRyRumVopR0pxES0Py1Z0
Public key 2: DB-6JedjTKz15R8280acYU07HAdU7TKqr-5p-Mx666Ya
Public key 3: DMEcEGpRWR02t8XXZ0r3ZYypq74ELc21n9aX03h_C
1. AAB0ervAG80Lyho99362UBTScec_4zY0VF1pJPM7MKb15TH60akvSvW60PC0Yx18Mcg8TW-Z3EhgC81I4A
2. ABB3c52ZbcE0dEma3E1CFUedsKqksU5T34CImGh3s0cs-k3dMcy2P3xQBejIvAet1-c271o1E-Mxq2-1CTN2aJ
3. ACBIeW08XvIxeqOuMc40b_-GuoF9e37TW8t60om-x8McSv8tHJp0p3EJH3bcz91H8bFuCRq0W4wyZ0T1p0c8
Signature 1 is valid.
Signature 2 is valid.
Signature 3 is valid.
ERR: Non zeroed prepad bits = 100000 in b's'.
Prefix: ELRpxQ2vo8plyhJfr9C0qR8l8jVaX0vxKwM0lFCT0ee1
Public key 1: DHA-515j88yMo11g_4XoFZmV3rG9gUfKXQHGtaJ7kb

ERR: Improper Habitat Interaction for pre=ELRpxQ2vo8plyhJfr9C0qR8l8jVaX0vxKwM0lFCT0ee1.
Prefix: ELRpxQ2vo8plyhJfr9C0qR8l8jVaX0vxKwM0lFCT0ee1
New Sequence No. 1
Public key 1: 0J1vnoWag8hepMGE159x3ad1sq9b5f5moU97srL2zj
Prefix: ELRpxQ2vo8plyhJfr9C0qR8l8jVaX0vxKwM0lFCT0ee1
New Sequence No. 2
Public key 1: 0ACePp0kxs82803xxQIPbo0m0eU4h4CKApryDhbFR4yb
Test Complete
```

Basic KLI for signing & verifying a message

```
# CREATE DATABASE AND KEYSTORE
kcli init --name test --nopasscode --salt 0ACDEyMzQ1Njc4Owxtbm9aBc

# INCEPTION EVENT
kcli incept --name test --alias trans \
--transferable --toad 0 --icount 1 --ncount 1 --isith 1 --nsith 1

# ROTATION EVENT
kcli rotate --name test --alias trans

# INTERACTION EVENT
kcli interact --name test --alias trans --data '{"data":123}'

# VIEW AID's KEL
kcli status --name test --alias trans --verbose

# SIGN ARBITRARY DATA
kcli sign --name test --alias trans --text 'abcdefghijklmnopqrstuvwxy'

# VERIFY ARBITRARY DATA
kcli verify --name test --alias trans \
--prefix EIryzWYlZ9bQr7EhMAoBXk4r2h-OgaEqERid7-AHNp6o \
--text 'abcdefghijklmnopqrstuvwxy' \
--signature AABorPTVJLp4vAOKyNwSP16QMqNI1nLCFKaPnifTmPmFTR0eLW0ZGuWuJtCvxXNiz0btV3dDsShCz3QM_Jb4MM
```

kcli init : Database and keystore initiation

```
kcli init --name test --nopasscode --salt 0ACDEyMzQ1Njc4Owxtbm9aBc
```

The name of the KLI database. KLI database is created either in `~/.keri` or `/usr/local/var/keri`.

A salt for generating key pairs using a hierarchical deterministic key (HDK) algorithm.

By default, the KLI database is encrypted and requires a passcode to use. The flag `--nopasscode` creates an unencrypted database.

kli incept : AID inception

The alias for the AID.

```
kli incept --name test --alias trans \  
--transferable --toad 0 --icount 1 --ncount 1 --isith 1 --nsith 1
```

- "transferable" sets whether the AID can be rotated.
- "wits" sets the AID's witness pool.
- "toad" sets the threshold of accountable duplicity.
- "icount" sets the number of current keys.
- "ncount" sets the number of next keys.
- "isith" sets the threshold for the current keys.
- "nsith" sets the threshold for the next keys.

The threshold of accountable duplicity (TOAD) is a threshold number M that the controller declares to accept accountability for an event when any subset M of the N witnesses confirm that event.

41

kli rotate & interact : Update KEL

```
kli rotate --name test --alias trans  
kli interact --name test --alias trans --data '{"data":123}'
```

Anchor arbitrary data to KEL

42

kli status : View KEL

```
kli status --name test --alias trans --verbose
```

s=0: inception event ("icp")

s=1: rotation event ("rot")

s=2: interaction event ("ixn")

```

{
  "v": "KERI10JSON00012b_",
  "t": "icp",
  "d": "E1ryzWYLZ9bQr7EhMAoBxk4r2h-0gaEqERid7-AHNp6o",
  "i": "E1ryzWYLZ9bQr7EhMAoBxk4r2h-0gaEqERid7-AHNp6o",
  "s": "0",
  "kt": "1",
  "k": [
    "DK1zX87vfaKLrB25LfEcKHt1IQwCacRsnZXiesQnhVve"
  ],
  "nt": "1",
  "n": [
    "E3e7Mrj1e5_0H1Qy49Bzurn1KKDaK4-z0PUhwrj_plfb"
  ],
  "bt": "0",
  "b": [],
  "c": [],
  "a": []
}

{
  "v": "KERI10JSON000160_",
  "t": "rot",
  "d": "E07KE15RveInYUzrDPrhLYzpgDTwEEvgEk2exxIQuRH0",
  "i": "E1ryzWYLZ9bQr7EhMAoBxk4r2h-0gaEqERid7-AHNp6o",
  "s": "1",
  "p": "E1ryzWYLZ9bQr7EhMAoBxk4r2h-0gaEqERid7-AHNp6o",
  "kt": "1",
  "k": [
    "0AZUzGSCJabcEC1ZFgy_uMnzeaz5VLSIYdXzoJhuoZWz"
  ],
  "nt": "1",
  "n": [
    "EP2YTjxQWZ6DeEB2kkmQkoLmuChxypGZjDK3px-udCj"
  ],
  "bt": "0",
  "br": [],
  "ba": [],
  "a": []
}

{
  "v": "KERI10JSON000d7_",
  "t": "ixn",
  "d": "EFtk2DR2CFxforZnHupsLDdt_DP68rjuwgC0pPP0b1u6",
  "i": "E1ryzWYLZ9bQr7EhMAoBxk4r2h-0gaEqERid7-AHNp6o",
  "s": "2",
  "p": "E07KE15RveInYUzrDPrhLYzpgDTwEEvgEk2exxIQuRH0",
  "a": [
    {
      "data": 123
    }
  ]
}

```

- "v" : version
- "t" : type
- "d" : digest
- "p" : previous digest
- "i" : identifier (AID)
- "s" : sequence number
- "kt" : threshold of current keys
- "k" : current keys
- "nt" : threshold of next keys
- "n" : next keys
- "a" : anchored data
- "c" : configuration
- "bt" : TOAD
- "b" : witness (backer) pool
- "br" : removed witnesses (backers)
- "ba" : added witnesses (backers)

kli sign & verify : Sign and verify digital signature

```
kli sign --name test --alias trans --text 'abcdefghijklmnopqrstuvwxyx'
```

Data to be signed by the AID's current key

```

kli verify --name test --alias trans \
--prefix E1ryzWYLZ9bQr7EhMAoBxk4r2h-0gaEqERid7-AHNp6o \ Signer's AID
--text 'abcdefghijklmnopqrstuvwxyx' \ Data to be verified
--signature AABorPTVJLp4vA0KyNwSP16QMqNI1nLCFKaPnifTMPMsFTr0eLW00ZGuWuJtCcxvXNiz0btV3dDsShCz3QM_Jb4MM

```

Signature to be verified

BC Gov Code With Us Results: AnonCreds in VCDM Format

Six Months Later

Agenda

- AnonCreds in W3C VCDM Format
- W3C VCDM Learnings
- Aries Impacts
- Development Teams:
 - DSR - AnonCreds Rust
 - Animo – Credo-TS
 - What's Cookin' – ACA-Py
- What's Next



BC DIGITAL TRUST

BC's Goals with this Work

- Maximum privacy preserving verifiable credentials
 - Unlinkability – no “super cookies”
 - Minimum data sharing for the business purpose
- Alignment with W3C Verifiable Credential standards
 - VCDM: [W3C Verifiable Credentials Data Model Standard](#)
- Open source development – BC is “open by default”
- Open a pathway to the next wave of privacy preserving credentials
 - AnonCreds, BBS+, whatever that will be...

AnonCreds to W3C VC Format, and Back

- Turns out, it's pretty easy...
- Done by moving around JSON
 - Signature on VC and VP contain identical **data** to AnonCreds Credential/Presentation
 - Canonicalization, signing, creating presentation, verifying presentation are all identical
 - All features of AnonCreds fully supported
- Supports parallel signatures
 - AnonCreds and NIST-approved Signature on the same verifiable credential
 - Aka – privacy and “less-privacy” perserving
 - Holder-Verifier determine which signature to use in what scenarios

AnonCreds ⇌ W3C

```
{
  "schema_id": "3av...s8W:2:fabername:0.1.0",
  "cred_def_id": "3av...s8W:3:CL:13:default",
  "rev_reg_id": null,
  "values": {
    "given_name": {
      "raw": "Alice Jones",
      "encoded": "728...2918"
    }
  },
  "signature": {
    "p_credential": {
      "m_2": "5783...397",
      "a": "203...785",
      "e": "259...767",
      "v": "626...819"
    },
    "r_credential": null
  },
  "signature_correctness_proof": {
    "se": "163...839",
    "c": "546...523"
  },
  "rev_reg": null,
  "witness": null
}
```

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://bit.ly/anoncreds-context",
    {
      "@vocab": "urn:anoncreds:attributes#"
    }
  ],
  "type": [
    "VerifiableCredential",
    "AnonCredsCredential"
  ],
  "issuer": "did:sov:3avoBCqDMFHFaKUHug9s8W",
  "issuanceDate": "2022-11-10T17:24:26Z",
  "credentialSchema": {
    "type": "AnonCredsDefinition",
    "schema": "3av...s8W:2:fabername:0.1.0",
    "definition": "3av...s8W:3:CL:13:default"
  },
  "credentialSubject": {
    "given_name": "Alice Jones"
  },
  "proof": {
    "type": "CLSignature2022",
    "encoding": "auto",
    "signature": "AAA...FLM"
  }
}
```

AnonCreds ⇌ W3C

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/security/data-integrity/v2",
    {
      "@vocab": "https://www.w3.org/ns/credentials/issuer-dependent#"
    }
  ],
  "type": [ "VerifiableCredential" ],
  "issuer": "did:key:z6Mk...WoT",
  "credentialSubject": {
    "height": 175,
    "sex": "male",
    "age": 28,
    "name": "Alex",
    "id": "did:key:z6Mk...Y1u"
  },
}
```

```
"proof": [
  {
    "cryptosuite": "anoncreds-2023",
    "type": "DataIntegrityProof",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "did:key:z6M...WoT/credential-definition",
    "proofValue": "ukg..."
  }
],
"issuanceDate": "2024-02-07T06:59:10.848067Z"
```

Interesting Details

- Limitation: AnonCreds first
 - Put any AnonCreds credential schema into JSON-LD
 - Not the other way around
 - Flat list of claims is flat – no arrays
- AnonCreds JSON-LD does not use RDF Canonicalization
 - Claims are encoded as integers, encoded integers are signed (no change)
- Using JSON-LD “vocab” for the credential schema
 - With the ideas that a JSON-LD context for the credential schema **could** be provided.

Interesting Details

- No new `@context`
 - Every AnonCreds-specific field goes into the `proofValue` – e.g., `schema`
- Tricky issue – what to do with a claim that is used in multiple predicates
 - Single predicate: `"age": true`, but what to do if asked for `age > 20` and `age < 65` in one request?
 - Decision – not allowed.
 - For AnonCreds v2, will have to address that.
- Proof encoding enumerated to cover three types of signatures – VC, VC in VP, and VP.

Interesting Details

- Credential Revocation
 - AnonCreds scheme has different requirements – unlinkability
 - Verifier is NOT given a unique credential ID to check (the RevRegID+Index of presented VC)
 - Holder creates Non-Revocation Proof
 - Implementation does not use `credentialStatus` entry
 - But could be included (unsigned in AnonCreds) for use in parallel signatures applications
- What to do with “issuance_date”?
 - Included in VC, but not used by the Holder – not disclosed in a presentation
 - Included in VP as the date/time of VP generation

Parallel Signatures

- VC Crypto-Agility via adding multiple types of signatures to a credential
- Goal: Flexibility / long term vulnerability protection
- Example: NIST-approved + AnonCreds + Quantum-safe

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://bit.ly/anoncreds-context",
    {
      "@vocab": "urn:anoncreds:attributes#"
    }
  ],
  "type": [
    "VerifiableCredential", "AnonCredsCredential"
  ],
  "issuer": "did:sov:3avoBCqDMFHFaKUHug9s8W",
  "issuanceDate": "2022-11-10T17:24:26Z",
  "credentialSchema": {
    "type": "AnonCredsDefinition",
    "schema": "3av...s8W:2:fabername:0.1.0",
    "definition": "3av...s8W:3:CL:13:default"
  },
  "credentialSubject": {
    "name": "Alice Jones"
  },
  "proof":
    { "type": "DataIntegrityProof",
      "cryptosuite": "eddsa-2022" ... },
    { "type": "CLSignature2022", ... },
    { "type": "PSLatticeSignature2025", ... },
  }
}
```

Providing Parallel Signatures

- Works with AnonCreds in W3C Format
 - Convert AnonCreds Credential to W3C VC Standard format, with AnonCreds Signature
 - Pass to another “sign” library to generate, add signature to VC
 - Result: Holder can use VC with AnonCreds or other Signatures
 - Generate an AnonCreds presentation, with all it’s privacy-preserving goodness
- Or,
- Present the VC using one or more LD-Signatures (losing all added AnonCreds capabilities)

Aries Impact

- Aries Issue Credential and Present Proof protocols impacted
 - How to (easily!) signal that AnonCreds VCDM is being used?
 - Model:
 - Protocols are the same regardless of the VC/VP Format
 - Attachment formats are used to handle the different formats
- Approach Implemented:
 - New “Issue Credential” format defined “VC-Data Integrity” for any VC-DI credential.
 - Existing DIF Presentation Exchange attachment used for VP
 - Change: Include AnonCreds credentials when searching.

<https://bit.ly/IIWAnonCredsVCDM>

BC Gov Code With Us's

- Hyperledger AnonCreds in W3C VC Format
- AnonCreds in W3C VC Format Support in Aries Cloud Agent Python
- AnonCreds in W3C VC Format Support in Aries Framework JavaScript and Aries Bifold



BC DIGITAL TRUST

<https://bit.ly/IIWAnonCredsVCDM>



BC Gov's Code With Us (CWU) Program

- Procurements open to anyone in the world to contribute to open source
 - Defined open source deliverable
 - Simple application process – pay attention to the “Procurement Evaluation Criteria”
 - Short timelines from announcement to application to award
- Extremely successful for BC Gov Digital Identity and Trust initiatives
- For AnonCreds in W3C VC Format – three Code With Us opportunities
 - AnonCreds Rust Implementation
 - Using AnonCreds Rust Implementation in Aries Cloud Agent Python
 - Using AnonCreds Rust Implementation in :Aries Framework JavaScript and Aries Bifold

Implementation Work

- [DSR Corporation](#) delivered the [AnonCreds Rust](#) features
- [Animo Solutions](#) delivered the functionality in [Credo-TS](#) and [Bifold Wallet](#)
- What's Cookin is wrapping up implementing the functionality in [ACA-Py](#)

What's Next

- For BC: Deployment in ACA-Py Issuers, Verifiers and the BC Wallet
- Ongoing transition to use the W3C VCDM in all implementations
- AnonCreds v2 (or a privacy-preserving equivalent)

AnonCreds v2 or Its Equivalent

- AnonCreds v2 exists as a proof-of-concept implementation
 - BBS+ or PS signatures as the underlying signature scheme
 - Additional encoding information in schema to enable key ZKP features
 - Existing: Selective disclosure, unlinkability, revocation, link secret for holder binding
 - New: Range proofs, set membership, domain proof, claim equality, verifiable encryption, blinded data
 - Work to be done:
 - Evolving/specifying data structures
 - must use W3C VCDM, must support arbitrary JSON schemas

Combining Efforts with other BBS+ Work

- Lots of other efforts towards the next generation of privacy-preserving verifiable credentials based on BBS+
- Our goal is to keep some of the opinions of AnonCreds in that work
 - Ease of use
 - Same objects (schema, definition, VC, request, VP)
 - Same interactions (Offer-Request-Issue, Request-Present-Verify)
 - Link secret-based holder binding
- Ambivalent on using RDF canonicalization
 - Will be using RDF/Linked Data in other efforts at BCGov...

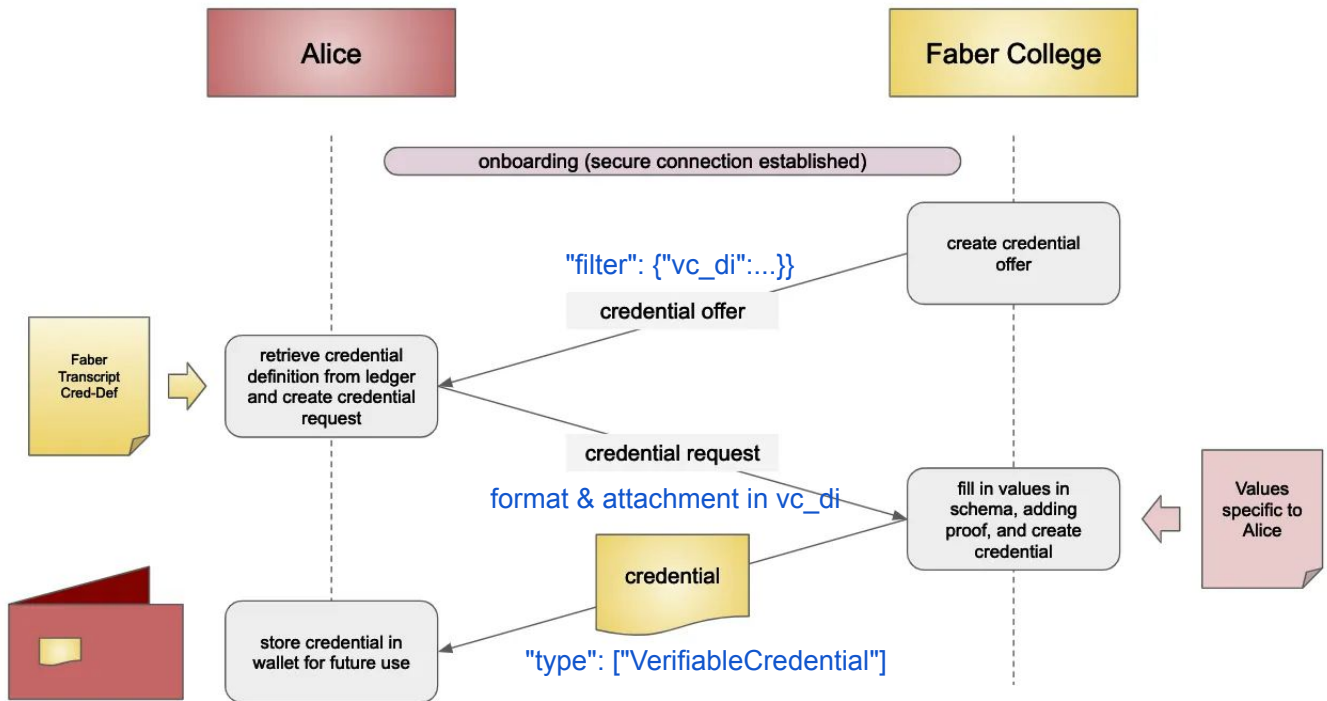
Discussion? Comments? Questions?

-

VC-DI: Verifiable Credentials with Data Integrity

What's Cookin: ACA-Py support for W3C compliant credentials

<https://bit.ly/HWAAnonCredeVCDM>



Credits: KC Tam : Exploring Hyperledger Indy through indy-dev Example

<https://bit.ly/HWAAnonCredeVCDM>

New Function Signatures and Handlers

```
async def create_credential_w3c
```

ACA-Py library users only have to set the filter on the credential offer request



Complexity of creating the new presentation format is kept "under the hood"

<https://bit.ly/IIWAnonCredeVCDM>

Team - new What's Cookin Aries and ACA-Py Crew



Thura Aung



Sarthak Vijayvergiya



Kenechukwu Orjiene