出國報告（出國類別：考察訪問）

西班牙全球資訊網協會年度大會(W3C TPAC 2023)交流出國報告

服務機關：數位發展部
姓名職稱：黃彥霖資安制度工程師
派赴國家：西班牙
出國期間：112.09.6-112.09.17
報告日期：112.09.25

摘要

數位發展部於2023年加入全球資訊網協會（World Wide Web Consortium, W3C），加速推動國內產官學社導入網路標準，強化網路發展與互聯環境，今年為第一次實際參與該國際組織一年一度的諮詢委員會與技術大會（Technical Plenary and Advisory Committee, 以下簡稱 TPAC）。全球資訊網協會成立近30年，主導許多國際重要標準，且成功成為大規模使用的標準語言，如超文本標記語言（HTML）、階層式樣式表（CSS）、網站無障礙規範（WCAG），目前各工作組也正在研發頒布許多次世代標準，如可信賴憑證（VC）、分散式身分（DIDs）等。全球資訊網協會作為多方利害關係人（multi-stakeholder）型態的國際組織，不同於多邊（multi-lateral）或單邊（uni-lateral）型態的國際組織須以國家身分參與，全球資訊網協會接受不同型態的法人參與，較具有靈活彈性以及國際交流空間，參與者具多元身分，如國家法人、國際大型企業、非營利非政府組織、學術單位等，有效促進網路環境能夠被友善討論。國內過去只有數位出版聯盟參與 W3C 事務，藉由數位發展部實質參與，希望長期而言能促進國內數位標準研發進度並且對接國際發展潮流，產生具有民主韌性的網路事務參與環境。適逢全球資訊網協會成立近30年，該協會為了順應國際發展趨勢，正在進行全面改組，以不同區域的學術機構主責該區域事務，並強化諮詢委員會成員（Advisory Committee Member）實質權力，此刻我們也積極參與各項事務討論，如董事會改選、技術架構組改選與總章程、各章程修訂等，實質達成國際交流之綜效。此外，於2023間，本部各單位持續參與各工作組線上會議以及代表會議，本次出席 TPAC 將成效與各國與會代表交流。未來網路環境將日益複雜，如何有效順應國際標準趨勢，將是刻不容緩的議題。

目錄

壹、參與目的

一、國際標準對接：數位發展部於今（2023）年1月以政府機關名義（Ministry of Digital Affairs, Taiwan）加入制定全球網路標準的國際組織「全球資訊網協會」，成為正式會員。W3C 成立於1994年，是全球資訊網路的主要國際標準組織之一，目的是透過促進開發可互通技術，致力於制定網路共通標準，使全球資訊網一體化。數位部擔任我國數位資訊政策統籌機關，其中一項重點工作即是透過參與跨國組織的合作，參與各種網路政策與標準的制定，以維護主張臺灣在數位網路領域的利益。自2023年4月以來，本部每個月辦理乙次 W3C 部內工作會議，與參與工作組的內部各單位討論推動進度等，本次參與國際會議目標之一為參考各國與各企業內部於早期參與草創階段，如何有效促進成員參與。

二、各工作組進度更新：目前本部（含數位政府司、民主網絡司等）與數位產業署、國家資通安全研究院等已實質加入13個小組，以及屬於組織管理層次的諮詢委員會（Advisory Committee），參與小組分別為無障礙指引工作組（Accessibility Guidelines Working Group）、分散式身分識別符工作組（Decentralized Identifier WG）、可信賴憑證工作組（Verifiable Credentials WG）、網頁應用程式安全工作組（Web Application Security WG）、隱私興趣組（Privacy Interest Group）、網頁支付工作組（Web Payments WG）、網頁支付安全興趣組（Web Payment Security Interest Group）、沈浸式網頁工作組（Immersive Web WG）、CSS 工作組（Cascading Style Sheets WG）、多樣化網際網路應用程式工作組（Accessible Rich Internet Applications WG）、開放式使用者介面社群（Open UI Community Group）、無障礙教育與推廣工作組（Accessibility Education and Outreach Working Group, EOWG）、ACT 規則社群（ACT Rules Community Group）等等。部內目前每個月舉辦工作進度會議，並持續以導入標準、研析驗證相關內容至臺灣網路環境為目標。

三、參與代表會議：本次參與一大任務為，以諮詢委員會代表之代理身分（Alternative AC Representative）參與半年度的諮詢委員會議（Advisory Committee Meeting）。此外也以各工作組成員身分參與各工作組會議，並與各 W3C 成員、W3C 組織員工、獲邀參與之技術專家交流。本（民主網絡）司目前主導國內分散式身分識別符標準（Decentralized Identifiers, DIDs）推動事務，全球資訊網協會於2022年7月發布了第一版分散式身分識別符標準（Decentralized Identifiers, DIDs），

此次 TPAC 適逢分散式身分標準發布後一週年，正在討論重整內容與改版，數位部參與其中可對齊國際趨勢。我們持續推「個人身分自主權」（Self-Sovereign Identity, SSI），在國際上討論第三代網路（以下簡稱 web3）等相關技術發展時，達成各網路平臺的「攜碼互通」服務，讓使用者有機會跳脫現在大型跨境平臺的網路圍籬，建置以個人需求為出發點的技術標準。本司今年根據 DIDs 標準於臺灣作為試驗場域進行研析與驗證，希冀以 web3方式結合隱私強化技術，並創造可信賴的跨境資訊交流。本年為 moda 以官方身分參與 W3C TPAC 第一年，就技術標準層次進行資訊交換，並討論國際數位趨勢，加速推動國內數位環境。

圖1 參與 AC 會議過程

貳、參與行程：

本次參與西班牙全球資訊網協會年度大會行程自 112 年 9 月 11 日至 112 年 9 月 15 日合計 5 日，行程安排如下表：

表 1 參與西班牙全球資訊網協會年度大會行程表

日期	活動內容
112.09.06(三)	● 啟程前往西班牙
112.09.11(一)	● 參加聯邦式身份社群組（Federated Identity Community Group）會議
112.09.12(二)	● 參訪分散式身份識別符工作組（Decentralized Identifier WG）會議 ● 參加聯邦式身份社群組（Federated Identity Community Group）會議 ● 參加諮詢代表會議（AC Meeting）
112.09.13(三)	● 參加技術大會（Technical Plenary）
112.09.14(四)	● 參加 Solid 社群組（Solid CG）會議 ● 參加可信賴憑證工作組（Verifiable Credentials WG）會議
112.09.15(五)	● 參加可信賴憑證工作組（Verifiable Credentials WG）會議
112.09.17(日)	● 返抵臺灣

參、參與概要：

本次為數位發展部第一次派員參與全球資訊網協會年度大會，本次以諮詢委員會代表之代理身分與工作組成員身分出席，參與各工作組、事務討論、以及技術大會。本次活動共5天，第3天為諮詢委員會會議，進行組織事務報告與討論；第2天為技術大會，除此之外皆為各工作組、社群組、興趣組等議程。以下段落先以「W3C 組織沿革與組織創新」進行統整分析，再以每日參與之會議為單位，羅列該會議組之介紹與參與概要。

簡要敘述 moda 作為 W3C 身分之會員權利，為與來自全球的法人和專家交流合作，這些參與者對網路具有長期影響力，藉由實體會議可直接討論協作與探索。所有 W3C 會員下的成員，都可以用個人身分參與任一 W3C 工作組、興趣組與社群組，各組近三十年來持續制定可持續的網路標準，並透過這些技術標準，讓網路使用者可以在符合普世價值的前提下使用網際網路，這些價值包括國際化（Internationalization, i18n）、隱私（Privacy）、安全（Security）與可及性（Accessibility, a11y，或譯為無障礙、親和力）；W3C 各工作組成員與諮詢委員能夠透過審查提案與參與 W3C 工作坊，為 W3C 提供策略方向，實現「世界是一個網路」的目標。根據本次參與的不同工作組，概要整理如下：

一、 W3C 組織沿革與組織創新

W3C 成立於1994年，是全球資訊網的主要國際標準組織之一，目的是透過促進開發可互通技術，致力於制定網路共通標準，使全球資訊網一體化。W3C 由提摩西・約翰・柏內茲—李爵士（Tim Berners Lee）成立，李爵士自從成功串連傳輸控制通訊協定／網際網絡通訊協定（TCP/IP）、超文字傳輸通訊協定（HTTP）、與超連結等三項功能後，成功建置全球資訊網的環境，此後放棄專利，於麻省理工學院（MIT）成立 W3C 維護與打造更多新協定，許多標準協定如今已成為網路共通標準。此後近30年來，該聯盟由各會員聯合組成，會費維持全職員工協助組織營運，並共同開發全球資訊網絡標準，到目前為止 W3C 擁有462名會員，活躍成員以大型跨境平台企業為主，如 Google、微軟、蘋果、Mozilla 基金會等。

此外 W3C 也塑造了平等協作的網路文化氛圍，各工作組內部並不因來自大

型企業、新創企業或非營利組織而有差別。事實上，參與者雖然皆來自成員組織（AC Member），但參與身分皆為個人，各組別基本上具有自主權，若有組內或組間爭議，才會交由技術架構組（Technical Architecture Group, TAG）或諮詢董事會（Advisory Board, AB）處理，而 TAG 與 AB 皆由所有成員組織選舉而成，此為多方關係人型態的國際組織常有的治理型態。工作組之組內成員通常藉由信件列表（Mailing List）、網際網路中繼聊天協議（IRC）、線上軟體原始碼代管服務平台 Github 進行協作。經年累月下來，W3C 已產生了一套標準建立流程，透過各工作組章程（Recharter）規範，工作組經歷「草稿（Working Draft, WD）—標準建議候選（Candidate Recommendation, CR）—標準建議提案（Proposed Recommendation, PR）—正式標準建議（Recommendation）」，交付正式的網路標準。如筆者參與之 DID 工作組自2019年開始撰寫草稿，經過三年，於2022年7月正式頒布「分散式身分識別符 v1.0」（Decentralized Identifiers (DIDs) v1.0）標準建議。

而自2020年代開始 W3C 面臨麻省理工學院退出營運，W3C 順勢進行國際層次的組織再造與重塑，其新版本的治理文件與願景白皮書分別可見於「W3C Process Document」與「Vision for W3C」，分別摘錄如下：

「W3C Process Document」文件於2023年11月正式公告，象徵組織再造完成，並規範組織成員與各工作專案行為。該文件描述 W3C 組織架構以及使 W3C 能夠完成其使命的流程、權責和功能。W3C 的工作目標為網路技術標準化，為了完成這項工作，W3C 制定各項技術標準建議書，促進會員、團隊和公眾之共識。W3C 的正式流程鼓勵共識、徵求評論（包括所有會員和公眾）、納入實作與可互通性等經驗，在技術報告的開發過程中獲得全體會員同意，促進技術決策的品質與公平性。W3C 的參與者包括其會員代表、團隊成員，以及受邀專家（Invited Expert），後者可以帶來額外的專業知識或代表更多利益相關者。團隊代表（AC Representative）既參與技術工作，也確保每個小組與 W3C 事務可以適當整合。W3C 的技術標準稱為 W3C 建議書（Recommendation），由其工作組開發，此外 W3C 也有其他類型的出版文件。W3C 擁有各種類型的小組；該文件規範設立章程（Charter）的工作組和興趣組，此外 W3C 也運營社群組與商業組。在其之上，W3C 正式成立 W3C 諮詢委員會（AC），每個成員都有一名代表，以及兩個由其成員選舉產生的監督小組：諮詢董事會（AB），協助解決組織範圍內的非技術性問題並管理 W3C 流程的演進；以及技術架構組（TAG），協助解決聯盟範圍內的

技術性問題。以下案例是 W3C 對特定網頁技術標準化的啟動參考：成員對特定主題產生興趣，透過在社群組中發展提案或在會員提交中提出想法來表達興趣。此外，W3C 團隊也尋找不同興趣議題，並協助組織工作坊，將人們聚集在一起討論 W3C 社群感興趣的話題。當有足夠的興趣產生積極的社群時，團隊會與會員合作起草擬議的興趣小組或工作小組憲章。W3C 會員審查擬議的章程，當 W3C 內部支持在議題上投入資源時，W3C 批准該小組成立，並開始工作。數位發展部也於今年參與 AB 與 TAG 選舉事務，並且完成複數章程更新（Recharter）審查工作。

「Vision for W3C」部分，該文件幫助世界理解 W3C 是什麼，它做了哪些事，以及為什麼這些事情重要。核心願景如下：一、網路屬於全人類；二、網路是為了使用者的利益而設計的；三、網路必須為其使用者提供安全；四、網路是「一個」可互通的全球資訊網路。「願景」特別闡述其運作原則，以及指導準則，摘錄如下：「全球資訊網最初被構想為一種分享資訊的工具，它迅速演變成人類社會的基礎建設，透過擴大對知識、教育、商業、社交、公共服務與娛樂等功能，網路已經引發了重大的社會變革。然而網路的驚人成功也帶來了許多未預期且不受歡迎的後果，這些後果對社會造成了傷害：開放性和匿名性孕育了詐騙、釣魚和欺詐行為；輕易收集個人資訊導致了商業模式搜集與販賣個資，而人們對此毫無察覺；快速的全球資訊共享讓錯誤資訊得以繁衍並被用於政治或商業利益。這已經分裂了社會並激起了仇恨。我們必須做得更好，必須採取措施，在所創建的標準中解決這些後果。科技並非中立，新科技賦予了新的行動與可能性，我們必須負起責任，正視我們工作的實際影響。W3C 的技術架構組致力於明確定義『網路倫理原則』（Ethical Web Principles），提升網路倫理完整的基礎。全球資訊網應該是包容的，尊重其使用者：一個支持事實勝於虛假、人民勝於利潤、人性勝於仇恨的網路。」

於本段最後討論 W3C 組織再造的隱憂與機會，在數位發展部加入 W3C 的同一週，W3C 於2023年1月脫離麻省理工學院，現以「全球資訊網協會公司」（World Wide Web Consortium Inc.）的身分運作，並與北京航空航天大學（中國）、ERCIM（法國）和慶應義塾大學（日本）成為合作夥伴，處理不同區域之事務。根據官方新聞稿所示，「W3C 諮詢委員會正執行『使命』專案並進行組織再造。我們的社群－包括我們的會員、非會員貢獻者、團隊，以及所有使用成果的人－將繼續

發展『使命』。我們的力量來自於全球的包容性與多樣性。這應成為繼續精進的最佳指南。」數位發展部加入 W3C 時，以 W3C Inc.為簽約對口，目前事務討論來自日本與美國區域為主，惟 W3C 一方面擴大發展區域在地事務，也產生地方分權之效應。W3C 中國作為 W3C 合作夥伴，已經大規模推動簡體中文語言使用區的技術標準導入，並鼓勵許多中國企業，包含大型企業與新創企業，參與開放原始碼開發與公開標準建置。臺灣作為繁體中文使用區，在 W3C 部分應持續投入資源，以利追趕進度。網路技術標準作為跨境使用的技術架構，往往比地緣的語言使用區範圍來得更廣，如何在繁體中文與簡體中文使用者之間維持獨立性、在國際開放標準的協作上維護使用者隱私與自主權，同時創造便利性，與臺灣數位發展環境相關聯，必須審慎面對。

二、 參加聯邦式身份社群組會議

此次會議分為參加聯邦式身分社群組（FedID CG）與 ActivityPub 兩種情境脈絡與規格，以下分別介紹兩者，整理自官方介紹與現場討論。

聯邦式身分（Federated ID）是一技術標準和使用案例，包括將使用者標識（Identifier）和使用者身分驗證服務（Verification），與提供使用者訪問的資源服務。提供「使用者標識」、「身分驗證服務」的組織通常稱為標識提供者，使用其服務的組織通常稱為信賴方。聯邦式身分是使網站、應用和 API 能夠將身分驗證外包給外部實體。

聯邦式身分可以讓身分跨平台互通，如果 B 和 C 將身分驗證外包，則具有實體 A 帳號的使用者無需建立新的使用者帳號和密碼，即可存取應用 B 和 C。有時我們稱為單點登錄（Single Sign-on, SSO），SSO 和聯邦式身分之間仍有區別。SSO 是聯邦式身分的一個屬性，使用者無需重新輸入資料即可訪問不同的 Web 應用或 API。聯邦式身分範疇更廣，可以在不同網域與服務中彼此互通。

使用聯邦式身分的類型與網際網路一樣非常多元。常見的做法是使用聯邦式身分來簡化帳號管理和訪問，允許使用者以身分供應商帳號登錄（例如使用 Facebook 登錄、使用 Google 登錄等）。企業也經常使用它來管理員工對公司資源的取用，大學使用聯邦式身分為學生提供多機構學術課程，提供對教育資源的共享訪問以及研究合作，金融機構也是如此。此外，它也經常用於軟體即服務業務

（SaaS）模型中。

聯邦式身分藉由簡化了使用者體驗的複雜程度，讓使用者不用一直辦帳號，降低了與密碼重用相關的安全風險，減少了使用者必須記住和管理的訪問憑證的數量，並促進組織間的關係和管理。但是跨系統的使用者身分也會引起隱私問題。雖然聯邦式身分系統的目標是方便使用者訪問線上資源，但由於這項標準與 cookie 等可能有關，有可能被濫用來跟蹤使用者，而無需他們同意或完全理解。為了解決這些問題，使用者代理組織正在改變他們與網路設定的互動方式，以防止對使用者進行不受控制的隱藏跟蹤。由於聯邦式身分通常利用這些相同的格式來交換必要的資訊以完成身分驗證流程，因此我們需要開發解決方案來解決這些隱私問題，而不會破壞聯邦式身分。

使用者代理正在探索各種與隱私相關的干預措施。其中包括棄用第三方 Cookie、控制對使用者端網路儲存權限、從連結中刪除某些參數（通常稱為連結修飾）以及限制網頁導向的功能。聯邦式身分識別通常依賴於這些相同的機制，因此為改進對最終使用者隱私的支持而進行的更改正在對聯邦式身分系統產生影響。由於最直接的變化是棄用第三方 cookie（已經在 Safari 和 Firefox 中部署，並公開計劃於2023年底用於 Chrome），因此聯邦身分社區組織（FedID CG）目前將大部分注意力集中在該更改的影響上。該小組正在努力在棄用第三方 Cookie 時保留聯邦式身分驗證。

第二部分為 ActivityPub，ActivityPub 是一種標準，它允許不同的網路應用程式進行交互，以便使用者可以彙集他們的資訊並跨網站、跨應用程式進行協作，甚至是執行不同軟體。雖然 ActivityPub 在2018年才被採納為 W3C 的官方建議，但 ActivityPub 協定已經在大量專案中實施，包括 Mastodon、Misskey 和 Pleroma 等平臺；去中心化的媒體託管和共享平臺，如 Funkwhale（音訊）、PeerTube（影音）和 Pixelfed（圖像）；Plume 和 WriteFreely 等部落格平臺；社交網路平臺，如 Friendica。ActivityPub 支援常見的社交網路活動，如關注、按讚、發文、留言。舉例而言，如果在 Mastodon.social 等 Mastodon 上擁有帳號，則可以在 WriteFreely 上關注某人，並在他們有新文章時接收更新。

本次新討論內容如下：

一、將擴展功能納入 ActivityStreams2.0 的過程

（ ProcessforIncludingExtensionsinActivityStreams2.0 ），目前正在草稿狀態。ActivityStreams2.0是用於表示社交數據的詞彙表，如[activity streams-core]和[activity streams-vocabulary]中所述。它被[activitypub]API 和協定使用。它被設計為可擴展的，以便發行者和消費者可以使用。擴展至少提供以下好處為支援特定興趣領域的專業詞彙、對最初發佈 ActivityStreams2.0時不常見的社交軟體模式進行建模、為 ActivityStreams2.0中已表示的模式提供替代術語或結構，以提高詞彙表的清晰度或易用性。任何發行者都可以定義 ActivityStreams2.0的擴展，並在已發佈的文檔中使用它。例如，發行者可以定義一個擴展，為使用者最喜歡的霜淇淋口味提供術語。

二、最近在聯邦憑證管理（FedCM）方面有了顯著的進展和討論。Nicolás Peña Moreno 代表 Chrome 團隊介紹了自上次 TPAC 以來的進展，包括 FedCM 的發布和基本 API 的展示。他強調，在使用 FedCM 之前，使用者必須先登錄到身分提供者（IDP）。在 FedCM 的示範中，Nicolás 展示了一個設置了 IDP 登錄的示範頁面，用來設置不同類型的 cookies。這個過程展示了如何使用 FedCM API 從 IDP 獲取權杖。此外也討論了 FedID 實際部署狀況，其中 Google Identity 服務是主要合作夥伴，他們正在對小部分使用者進行 API 測試。雖然目前使用量不大，但預計隨著 Chrome 逐步淘汰第三方 cookies（3PCs），使用量將顯著增加。再來是大規模部署，FedCM 最初只能在頂級網站調用，但現在允許在 iframe 中使用。IDPiframe 可以顯示使用者之前選擇的帳號圖像，以個人化登錄按鈕。Mozilla 和 Brave 瀏覽器分別介紹了他們的部署狀況。Mozilla 在其預覽版本中只部署了一般版本，而 Brave 目前在 Chromium 中禁用了這個 API，並考慮修改 UI。身分錢包（Identity Wallet）互動和未來討論也是會議的一部分。參與者展示了一個原型 Android UI，允許選擇憑證，並討論了未來有關錢包互動的計畫。隱私和使用者意圖問題也受到了關注，PING（隱私興趣小組）計劃討論一些常見的隱私和自由表達方面的關注。

圖1 參加聯邦式身分社群組會議

三、 參訪分散式身份識別符工作組會議

分散式身分（DIDs）為本司今年的重點業務，藉由參與國際活動，交流各組織實施分散式身分的具體方法，並討論潛在合作的可能性。以下簡要敘述分散式身分介紹，內容整理自分散式身分識別符（DID）W3C 推薦標準文件。分散式身分是一種新工具，使網路上的每個人都能獲得尊重隱私的線上身分。在歷史演革上，最初，這些由行動營運商擁有「手機號碼」並「出租」給個人。這要求每個人在更換運營商時更改號碼。隨著手機號碼有了「可攜碼」的功能，每個人現在可以在更換運營商時「隨身攜帶他們的號碼」。如今，大多數電子郵件位址和社交網路位址也是如此——它們不是由個人「擁有」的，如果個人更換提供者，則必須更改。相比之下，W3C 分散式識別符可以由創建它們的個人或組織控制，在服務提供者之間是可移植的，並且可以持續到他們的控制者想要繼續使用它們。此外，DID 具有獨特的屬性，使控制器能夠使用加密技術驗證 DID 的擁有權。這

可以使 DID 的任何控制者（個人、組織、線上社群、政府、物聯網設備）能夠線上進行更值得信賴的交易。特別是對於個人來說，DID 可以讓他們重新控制自己的個人資料，並實現更相互尊重的雙向信任關係，防止偽造，尊重隱私，並增強可用性。從根本上說，分散式識別符是一種新型的全球明確標識碼，可用於識別任何主題（例如，個人、組織、設備、產品、位置，甚至是抽象實體或概念）。每個 DID 解析為一個 DID 文件，其中包含用於控制 DID 的加密材料和其他數據。DID 規範的基本支柱是：一、DID 不需要中央發卡機構（分散），二、DID 不需要底層組織的持續運作（持久），三、對 DID 及其相關資訊的控制可以通過加密方式證明（可驗證），以及四、DID 後設資料可以被發現（可解析）。

W3C 去中心化標識符與 W3C 可驗證憑證相結合，正在許多關注身分和數據真實性的市場中使用：各國政府－美國、加拿大和歐盟正在探索使用 DID 為其企業和居民提供保護隱私的數位身分檔，使這些實體能夠選擇共用其數據的方式和時間；零售商－美國的便利店、雜貨店、餐館、酒吧和消費品公司正在利用 DID 進行新的數位時代驗證計畫，以提高隱私、結帳速度，並打擊在購買有年齡限制的產品時使用欺詐性身分證件。供應鏈利益相關者（全球政府監管機構、貿易標準機構、供應商、託運人和零售商）正在使用 DID 來探索下一代系統，以更準確地驗證產品和服務的原產地和目的地，這將簡化並實現關稅流程、防止傾銷等問題。而大學、職業培訓計畫和教育標準組織也正在採用 DID，以頒發由畢業生在申請高等教育或勞動力職位時控制和共用的數位學習證書。

本次會議討論包含兩者，章程修改爭議，以及解析文件進度的推進，此外不同組織也有現場展示使用 DID 作為標準的概念服務。DID 章程修改部分，群組正在面臨標準化與包容性之間衝突，雙方的立場是在 DID 列表上，需要寧缺勿濫，還是包容最多的 DID 方法。目前正在尋找共識，待正式反對意見（Formal Objection）上交技術架構組以後，DID 工作組的管理人將會提出修正意見，並修改章程。此外在解析的部分，可驗證憑證和去中心化識別符號自從被 W3C 推薦發布後已獲得顯著的動力。這次分組會議的目標是提供對這些技術的快速介紹，並展示它們的一些部署情況。去中心化識別符（DID）是一種用於可驗證的「自主」數位身分的新型識別符。DID 完全由 DID 控制器控制，獨立於任何集中式註冊表、身分提供者或憑證機構。DID 解析器（Resolver）使用 DID 文件，這些簡單的文件描述了如何使用該特定 DID。DID 解析器獲取給定 DID 位址的 DID 文件。這是對

任何 DID 執行的四個必需操作之一（其他操作包括「創建」,「更新」和「停用」)。這些操作的細節根據 DID 方法的不同而有所不同。在 DID 解析的基礎上，DID URL 解引用是為一段過程，給定 DID URL 檢索資源。能夠執行這些過程的軟硬體稱為 DID 解析器。本規範定義了 DID 解析和 DID URL 解引用過程的共同要求、算法（包括其輸入和結果）、架構選項和各種考慮因素。

在 DID 大規模使用案例中，包含美國國土安全部的矽谷創新專案（DHSSVIP)，應用於美國公民及移民局、海關及邊境保護局。此外 DID 還與北美充電標準（NACS）有關——美國有15萬家商店，每天進行5000萬次年齡核查。最近，加州在其數位駕照中引入了 did:web 和 did:key。其他案例也包含 Microsoft Entra 已驗證身分。

四、 參加諮詢代表會議（AC Meeting）

作為新的 W3C 會員，moda 的諮詢委員會代表為唐鳳部長，稱為 AC 代表。AC 代表是會員與 W3C 之間的介面，執行作為會員組織的決策。AC 代表可以指定一名諮詢委員會代表之代理身分來分攤工作。W3C 的工作場域不僅重要且多樣，新進會員如 moda，可透過國際 W3C 團隊進行引導，在 TPAC 大會現場稱為 Team Buddy，本次由日本慶應義塾大學方的 W3C 員工 Naomi 協助接待。AC 代表能直接參與工作組，也能改派其組織其他人員到任何 W3C 組別。AC 代表既是機構的代表，也是 W3C 的會員組織傳達者。W3C 的資訊傳播模式有四種：當規範準備好進行實施時，AC 代表會收到通知；AC 代表應審查新的工作章程（WG Charter)，並進行投票；AC 代表針對 W3C 正式建議進行投票；AC 代表提名並選出董事會（AB）和技術架構組（TAG）的代表。而年度 AC 會議可以在現場討論與對齊決議事項，以下整理 AC 會議可公開之討論結論。

大會討論部分，創辦人李爵士正式從組織內部的協調者離開，重新成為自由的參與者。目前他主要集中工作於他自己發起的 Solid Protocol 事務。再來是 W3C 現況摘要：今年是 W3C 正式進入組織改組第一年，執行長即將公佈，2024年 TPAC 將在廣島與美國舉辦。另外大會主席也提醒章程的重新批准過程，希望 AC 代表踴躍參與，包含無障礙工作組、網頁元件工作組等等。關於無障礙工作組部分，網頁可及性規範已正式公告2.2版，並提供了許多免費的線上課程，歡迎參與者踴

躍提供意見與使用。此外還有 AI 相關的工作，包括 Web 神經網絡 API 和 AI 的道德和影響。講者提到了 Web 機器學習工作組的工作，以及關於 AI 對 Web 的影響的問題，包括內容生成和中心化風險等問題。最後是有關隱私工作，包括隱私興趣組和隱私原則工作組。講者提到了隱私工作組的問題以及如何解決它們

再來是技術架構組摘要，聯合主席介紹了 TAG 的職責和目前的工作，由於今年改組之後，TAG 的工作量與權力皆提高，包括審查其他人的工作，主要是設計各組架構，以及撰寫規範文件。TAG 目前正在進行隱私和安全相關問卷。所有人都可以在 GitHub 上參與設計審查，並建議有興趣的人可以開始參與設計審查和討論，以了解 TAG 的工作過程。近期將進入 TAG 選舉，選出改組後的 TAG 增額人選。

再來 AC 會議討論了 W3C 相關價值，如願景（Vision，已詳述於前），網頁倫理部分（Ethical Web Principle），是支持 W3C 技術工作的所有倫理原則。這份文件還在草稿狀態，接下來會更廣泛的共同審查。這份文件的意義在於，這是 W3C 首次嘗試的聲明，並希望能夠確保 W3C 的工作與這些原則一致。再來是隱私原則，一些新觀念是資訊流需要集體管理、支持自主權、最小化使用者數據、資料的敏感性、資料隱私權、去識別化數據等。這些原則的結構將幫助工程師在 API 設計中考慮倫理因素。

此外 AC 會議有討論了新興領域議題，如人工智慧的道德。講者強調了在 AI 解決方案中遵循和融入道德原則的重要性，以確保公平性。她提到了 W3C 的指南，並呼籲這些原則應該容易獲得，不應該存在障礙。她還談到了未來可能涉及可持續性和法規等問題，並呼籲大家參與討論。再來是「如何讓使用者控制其個人資料？」講者討論了如何讓使用者對其個人資料的使用具有控制權和透明度。他提到，雖然有《一般資料保護規則》（General Data Protection Regulation, GDPR）等規定，但使用者仍然感到對其數據的處理失去了控制。他談到了 Solid 專案，該專案旨在建立個人資料存儲服務器「pods」的規範，以實現更公平的數據治理平衡。他呼籲大家參與這項工作，並檢查其 GitHub 上的提議章程。再來是「可持續 Web 指南」（Web Sustainability Guideline, WSG），講者介紹了可持續 Web 指南的工作。他談到了氣候危機，並提到了該 CG 致力於制定可持續 Web 設計指南，以應對氣候危機。這些閃電演講涵蓋了多個主題，包括道德 AI、個人資料隱私、Web 性能優化和可持續 Web 設計。

五、 參加技術大會（Technical Plenary）

過去 W3C 的技術大會為集中化的演講大會，所有的與會成員、組織代表與技術專家共同在大講堂聽取不同主題的會議。但是自從有成員提議雙向交流遠比單向式資訊佈達還要重要以後，技術大會便改制為分散式的主題工作坊，在不同的會議室中，參與者可以選擇有興趣的主題，自由參與討論，技術大會同時開放給非正式成員參與。這次選擇有關「憑證」相關主題的議程參與討論，並在人工智慧道德的議程中，發表臺灣數位發展部與集體智慧專案（Collective Intelligence Project）於臺灣合作的具體情形。以下根據不同議程進行簡要介紹。

一、可信賴網際網路（Trustable Internet）：由慶應義塾大學提出的次世代網路概念，網際網路已成為社會和經濟活動的重要組成部分。手機和社交網絡服務的廣泛使用使個人和組織能夠隨時隨地發送和查看全球範圍內的數據。某些資料包含虛假資訊，可能引發社會問題。在許多情況下，查看者無法確認網際網路上數據的可信度，因此即使對虛假資訊存在懷疑，他們也只能對可信度做出自己的判斷。如果數據包含不確定內容，則基於此類數據做出的決策可能不準確。傳統上，數據的真實性是通過在每個單獨的系統中嵌入跡象來確保的，例如文件批准管理系統和包裝跟蹤系統，或者通過在網際網路以外的方式在數據發送方和接收方之間建立信任。為了在一般情況下使用這種方法，需要具備判斷網際網路上數據可信度的系統。然而，如果不影響網際網路現有的結構，要實現這一點是困難的。

因此，名為「可信網際網路」的架構在網際網路上疊加了一個層，具有確認數據可信度的機制，以便不影響現有的網際網路，並且網際網路使用者可以像以前一樣使用 Web、應用程式。該架構具有一個提供界面以存儲和共享「認可」資訊的認可層，該資訊是數據可信度的基礎。此外，它具有一個包含表示與數據相關聯的附加資訊的數據結構的認可圖。用於可信度判斷的附加資訊包括來自網際網路以及由人或物件添加的物理空間的資訊，這些資訊在生成數據後或生成後由人或設備提供。

在瀏覽網際網路上的數據時，可以根據需要從各種角度確認附加資訊，並且考慮到個人的主觀性，將資訊疊加在瀏覽器上。它還通過指出認可圖中資訊的缺乏來提高網際網路上數據的可靠性，並允許添加新資訊。將覆蓋到網際網路上，

可以實現一種通用方法，確保數據的可信度，而不影響傳統系統，這使得可以將可以確認網際網路上各種數據的資訊添加到其中。查看者還可以獲取能夠確認數據可信度的附加資訊，並根據該資訊進行主觀判斷。目前，人們只能通過個人判斷網際網路上數據的可信度，但在物理空間中的數據以及相關的附加資訊的支持下，可以從各種角度確認數據的可信度，並更準確地做出決策。這有望防止不可靠數據的使用以及虛假資訊和假新聞的再傳播。此外，通過擴大判斷範圍，將擴大經濟和社會活動的範圍，並實現社會的最佳方法。例如，當需要迅速判斷災害等情況時，可以提供必要的資訊。

二、可信賴網絡（Trusted Web）：同樣也是由慶應義塾大學提出的觀點，與前述網際網絡稍有不同，相對輕便的網路協議。在社會和經濟活動數位化的過程中，出現了各種問題，包括對假新聞和潛在社會分裂的擔憂，侵犯隱私，過度依賴某些在優勝者通吃情況下的服務，以及未充分利用的孤立工業數據。當社會正在過渡到「數位社會」時，目前的網際網路和 Web 通訊協議未能確保社會活動中的信任關係和安全感。因此，我們必須在網際網路和 Web 上重建信任。在當前的信任框架中，數據交換的可驗證領域有限，這使我們別無選擇，只能相信數位平台運營商等，而不檢查支持事實。我們還依賴它們提供的標識符機制來連接數據。有必要在不過度依賴某些服務的情況下，使用者能夠自行控制數據；在數據交換和追蹤中納入共識建立機制；擴大可驗證的領域，從而提高信任品質。

可信賴網絡旨在網際網路和網頁上覆蓋這種新的信任框架，以使各方能夠創建新的價值。透過可信賴網絡建立數據交換的信任框架對於促進業務之間的協作至關重要，這是數位轉型的基礎，要求跨部門和組織邊界實體的價值共創。架構設計部分，慶應講者分析了三個使用案例，包括個人（更換工作）、公司（申請補助）和供應鏈（交換化學物質含量數據）。此外，基於個人使用案例，他們開發了一個原型，以確定實現可信賴網絡所面臨的問題。在此基礎上，其中實體可以使用外部連結的身分管理系統來管理自己的身分。數據的可驗證性主要是通過數位簽名技術來實現的。整個數據集，包括簽名，可以通過驗證「簽名本身」、「簽名者」和「簽名意圖」來確認。數據交換過程的可驗證性是通過建模交換並結合數位簽名技術來實現的。當數據與其他各方交換時，其過程會相互記錄，以實現可驗證性。架構需要具有高度的靈活性，以結合標準和協議。講者預計，隨著提供了具有可信賴網絡所追求功能的各種服務，其使用領域將擴大，例如，在

運輸和個別服務層之間，將形成一種中間層。他們預計在中間層中，將確定應該兼容的 API、數據模型和協議，並且這種兼容性將確保互通性，從而實現標準化，促進將信任的 Web 建立為基礎設施。

三、身分錢包與網頁（Identity Wallets and the Web）：講者就隱私網頁工作組的示範案例，討論了國際標準組織（ISO）的 Mdoc 標準、W3C 的可驗證憑證（VC）和歐盟身分基礎架構（eIDAS2.0）在歐洲的立法情況。他談到了可驗證憑證的三方系統，包括發行者、持有者和驗證者，以及它們的應用場景，如美國移民局的疫苗卡、永久居民卡、工作應用、年齡驗證等。他還提到了一些潛在風險和問題，如信任發行者、隱私問題、設備控制等。在使用案例方面，會議討論了錢包資訊公開和調用的問題，開放一直是重要的問題。其中還包括許多應用案例，如金融服務、地址驗證、身分認證、安全的線上示範等。同時，還討論了可能的風險，如隱私問題、真實姓名政策、強制使用等。最後，該會議還討論了網頁瀏覽器在錢包生態系統中的角色和範圍，以及可能的影響和技術要求。講者表示，Chrome 只想成為網站和認證錢包之間的連接，不想成為錢包本身。總的來說，會議討論了可驗證憑證和錢包生態系統的各個方面，包括應用案例、風險和技術要求。這些討論將有助於推動相關標準和協議的發展和實施。

圖3 參與技術大會

六、 參加 Solid 社群組（Solid CG）會議

SolidCG 管理社會關聯資料協定（Social Linked-data Protocol,簡稱為 Solid

Protocol）進程，由李爵士提出，預定於2024年近一步成為工作組，成為正式協定，其目標與網際網路本身的目標一致：促進公平、資訊豐富和互聯的社會。Solid 透過擴展現有的 Web 標準，實現了一個個體可以保持自主性、控制數據和隱私，並選擇滿足自身需求的應用程式和服務的空間。目前各國政府與企業開始以 Solid Protocol 作為促進「個人自主權」的試驗。國外最知名的案例為比利時法蘭德斯地區，國內部分，中華電信有做過初期的概念驗證案例。為了對社會產生正面的利益，社群組使用了 W3C 之《道德網絡原則》來指引方向。

Solid 生態系統的一個主要設計目標是具有可演進性，並以安全和尊重隱私的方式為分散式 Web 應用程式提供基本的交換資訊能力。在這個環境中，參與者為其內容分配標識符，根據自己的訪問權限塑造和存儲數據，設置訪問控制，並使用首選的應用程式和服務來實現這些目標。這場 Solid 社群組的討論中，社群成員討論 Solid Protocol 與隨附章程的工作進度。

李爵士先發明了網路（www）與網頁及瀏覽器，然後發起 W3C，以治理各式網路標準，如 html、css、xml 等等，然後這幾年又在 W3C 裏面發起了 Solid 社群組，意圖使網際網路導回最初的模樣—去中心、互通且不分裂的網路。Web3.0最早的定義是語意網路（Semantic Web），而非區塊鏈。確實李爵士在討論會也提了一樣的事，畢竟這是他很久以前提出的，目前全球針對這個歧異語，初步共識是前者為 Web3.0，後者為 web3。Web3.0是一個更大的去中心互通敘事，不一定是區塊鏈或分散式帳本技術衍生的網路社會。而語意網路最近使用的人變少了，取而代之的是關聯資料（Linked Data, LiD），而 Solid 便是社交關聯資料（Social Linked Data）的縮寫。

他說 Web1.0透過 HTTP、HTML、CSS 與 RDF 等協議支援，由資料組合而成靜態網路。而 Web2.0新增了 JavaScript 與 web APIs 等功能，讓互動的網頁應用程式成為可能。但這些應用程式通常典型的架構是在伺服器與 app 之間溝通，如 Facebook。Web2.0的網頁資訊是不可互通的，如使用者資料。而有了 Solid 協定，你可以用 Solid 登入任何一個服務，如 Google。而 Web3.0意圖將這個互動性還給使用者，築牆自保，再談互通，而非將資料暴露於豺狼虎豹之中。

Solid Protocol 基本分成三個層次：關聯資料格式（Linked Data, LiD）、身分（webID）與倉庫／保險箱（Pod）。在理想世界中，你的所有資料是存在保險箱裡面的，你可以自己弄一個保險箱，也可以用別人的保險箱服務。而這些保險箱

都可以用 webID 來打開與控制別人能否打開。這與臉書或 Google 完全不一樣了，因為資料是在自己身上的，別人只能看到「資料的資料」，也就是關聯資料（LiD or metadata）公開展示。直到使用者同意臉書使用資料，臉書才能使用真實的個人資料，並讓個人繼續在保險箱裡面添入資料。

這與現在常見的網路使用方式完全不同。因為資料與個人身分是由自己掌管的，一言不合就可以遷移到其他服務上，而不是被單一服務商給綁架。其實目前已有懷著類似理想的人進行不同工作，如社交平台互通的 ActivityPub 或 Fediverse、去中心身分（Decentralised Identity）與去中心社會（DeSoc）（該流派也提出以靈魂綁定代幣（SBT）處理社交圖譜與社會信用，如 zkSBT），或歐盟三項協定如 eIDAS（電子身分與信用服務）EUDI（歐盟數位身分錢包服務）與 EBSI（歐盟區塊鏈基礎架構）。

目前 SolidCG（社群組）已經寫好新章程，即將再下一城升格為 SolidWG（工作組），讓我們繼續觀查這個充滿學術風味的 Web3.0，能否真的保護人類的數位身分自主權、資料民主與資料聯盟。此外，該會議中，不同政府表示已經針對 Solid 協議，進行個人資料儲存授權的驗證服務，李爵士也是英國政府數位化的重要推手，Solid Protocol 的國際使用情形，值得我們持續關注。

七、 參加可信賴憑證工作組會議

可驗證憑證工作小組（Verifiable Credentials Working Group, VCWG）（原稱可驗證主張 Verifiable Claims）的使命是在網絡上更輕鬆、更安全地表達和交換經第三方驗證的憑證。該工作組提出可驗證憑證（VCs）標準，是一種開放標準的數位憑證，可以代表物理憑證中的資訊，例如護照或駕照，以及純數位的內容，例如銀行帳號的所有權。與傳統的物理憑證相比，VCs 具有多項優勢，其中最重要的是其具有數位簽名，確保資訊不會被篡改，並且可以即時進行驗證。此外，VCs 的可用性也面臨一些問題。任何人都可以發佈 VC，並且可以包含各種資訊，這可能導致憑證的濫用。VCs 的生態系統涉及到三個主要實體：發行者（Issuer）、持有者（Holder）和驗證者（Verifier）。發行者創建並簽署憑證，然後將其交給持有者，後者將其儲存以供需要時使用。持有者可以通過向驗證者展示其憑證，來證明其所宣稱的資訊，實現資訊的驗證過程。因此信任模型（Trust Model）如下，

可驗證憑證的持有人位於信任三角的中心，調解發行方和驗證方之間的關係。三角形中的任何角色都可以由人、機構或機器扮演。發行人信任持有人，持有人信任驗證者，而驗證者信任發行者。

VC 模型將憑證持有人置於身分生態系統的中心，使個人能夠完全掌控其身分屬性。W3CVC 模型類似於實體憑證：使用者持有憑證，可以在需要時自主展示，無需事先通知或獲得憑證發行者的許可。這種模型是分散式的，賦予參與者更大的自主權和隱私保護。這與採用安全性聲明標記語言（SAML）和 OpenID Connect 的聯邦身分管理（FIM）模型形成鮮明對比，後者將身分提供者（IdP）置於中心地位，充當身分屬性的分發者，並決定哪些服務提供者（SPs）可以獲取這些屬性。在聯邦模型中，IdP 了解使用者訪問的每個 SP。

關於標準文件部分，W3C 於2019年11月19日發佈《可驗證憑證資料模型1.0-在網路上表達可驗證資訊》，該模型旨在實現身分資訊的分散式管理和在網路上的安全傳輸。此外尚未發布的規範性文件包含「可驗證憑證數據模型2.0」（Verifiable Credentials Data Model, VCDM 2.0）與「保護可驗證憑證1.0」（Securing Verifiable Credentials, SVC1.0）、「資料完整性」（Verifiable Credential Data Integrity 1.0, VCDI），此外還有用於數據完整性的加密套件：JSONWeb2020、EdDSA、NISTECDSA、Koblitz ECDSA 等等。以下簡要敘述兩日討論結論。

第一日

一、可驗證憑證數據模型（VCDM）是一個旨在實現可驗證的數據模型的標準，目的是提高數據交換的安全性和可信度。在 VCDM 的開發過程中，已經提交了多個 Pull Request（PR），以改進和擴展該標準。這些 PR 包含了針對 VCDM 規範的各種改進和修正，並在開發團隊中進行審查和討論，以確保最終的規範能夠滿足各種需求並保持高度的可信性。這些 PR 涵蓋了不同方面的改進，包括上下文處理、JSON-LD 解釋、術語定義等，所有這些都是為了更好地實現 VCDM 的目標。這些 PR 的合併和審查過程正在積極進行中，以確保 VCDM 的不斷發展和改進。

二、關於語言支援的討論：討論了在 VC 中如何支援多語言文本以滿足國際化需求的問題。討論了多種不同的選擇，包括使用 JSON-LD 的語言功能以及是

否使用@符號。最終，決定採用使用@value，@language 和@direction 關鍵字，並將它們別名為 lang_value，lang_language 和 lang_direction，以避免@符號引起的困惑。此外也討論了驗證與核驗的區別：討論了驗證和核驗在 VC 數據模型中的含義以及它們之間的區別。有關國際化審查的討論：討論了有關如何處理語言支援的問題，包括使用 JSON-LD 的語言功能以及多種不同的選擇。

三、資料完整性（Verifiable Credential Data Integrity 1.0, VCDI）：本規範描述了使用加密技術確保可驗證憑證和類似類型受約束數位文件的真實性和完整性的機制，特別是通過使用數位簽名和相關數學證明。本規範描述了使用加密技術確保可驗證憑證和類似類型受約束數位文件的真實性和完整性的機制，特別是通過使用數位簽名和相關數學證明。加密證明支援對分散式系統的實現者有用的功能。例如，證明可用於：在不失去信任的情況下可以共用聲明，因為它們的作者身分可以由第三方驗證，例如作為可驗證憑證[VC-DATA-MODEL-2.0]或社交媒體貼文的一部分。作為由特定識別符的實體進行身分驗證，例如，作為由分散式識別符（DID）標識的主題進行身分驗證。通過授權功能[ZCAP]等機制，在遠端執行環境中委派操作的授權。此外，許多基於加密數位簽名的證明提供了完整性保護的好處，使文件和數據不可篡改。

四、VCJSON：其中包括 VC JSON Schema、VCDM（Verifiable Credentials Data Model）的問題、VC-JOSE-COSE（虛擬認證 JSON Object Signing and Encryption）等。首先，討論了 VC JSON Schema 的相關議題。Gabe Cohen 提出了有關 JSON Schema 的工作概述，並提到了兩種類型的 JSON Schema，即 Json Schema 和 Json Schema Credential。討論還包括了對規範參考的調整，以簡化進入候選推薦（CR）階段的過程。最終，提出了讓 Verifiable Credentials JSON Schema 規範進入 CR 階段的提案。接下來，討論了更多關於 VCDM 的問題。其中包括有關如何處理 VCDM 中尚未解決的問題，以及關於證據擴展點的討論。然後，討論了 VC-JOSE-COSE 的相關議題。其中包括有關添加對 DID（去中心化身分識別符）的支持、刪除 JWT 引用、關於 kid（key identifier）的討論，以及其他有關 JOSE（JSON Object Signing and Encryption）規範的議題。最後，討論了其他 JOSE 和 COSE（CBOR Object Signing and Encryption）規範的議題，以確保虛擬認證的安全性和互操作性。許多問題需要更多的討論和明確的指引，以確保各種實現都能正確地使用虛擬認證。

五、第一日決議：決議#1：要求發布「可驗證憑證數據完整性1.0」規範；決

議#2：要求發布「數據完整性 EdDSA 加密套件 v1.0」規範；決議#3：要求發布「數據完整性 ECDSA 加密套件 v1.0」規範；決議#4：要求發布「可驗證憑證 JSON Schema」規範。

第二日

一、VC-狀態列表：VC-Status List 是一個處理身分驗證憑證狀態的規範。這個議題是關於 VC-Status List 的許多具體問題和決議。問題涵蓋了 VC-Status List 的各種方面，包括是否應該使用 Base64或 Base64Url 進行編碼、是否應該在更新時添加「雜訊」以保護隱私、以及如何定義詞彙和屬性等。其中也包含是否應該設定最小位數、是否應該使用 HTTP 狀態碼、以及如何處理隱私問題。目前 VC-Status List 的發展和設計仍在進行中。未來可能會有更多的討論和決策，以確保其正確運作和安全性。

二、網路孵化器社群組與網路錢包：社群組與 Chrome 團隊的代表討論了他們與網路錢包和身分憑證相關的目標和計劃。Chrome 的目標是在網路錢包和身分憑證的背景下啟用錢包發現和調用，幫助網站從錢包請求憑證；支持多個錢包，Chrome 的目標是使使用者輕鬆擁有多個錢包；重視隱私，希望在調用錢包之前獲得有意義的同意；跨設備請求，實現無縫的跨設備請求，如通行證；促進競爭和選擇：Chrome 希望避免偏袒某個錢包或憑證格式，並實現讓發行者和使用者選擇最適合自己的方式。從過去經驗可知目前有格式不可知性的議題，儘管最初 Chrome 專注於 mDL（數位駕照），但 Chrome 目前的原型不受格式限制。他們希望同時支持各種格式，包括可驗證的憑證（VCs）和 mDL。此外 Chrome 打算與現有的憑證管理 API 集成，以允許使用者從多個提供商中選擇。他們希望確保當網站請求身分憑證時，使用者應使用哪個錢包是清晰的。Chrome 不打算偷窺錢包內部；他們假設使用者已經選擇了可信任的錢包。他們的威脅模型不包括惡意錢包，並且依賴於使用者的選擇和應用商店的政策來維護信任。工作計劃在網路孵化器社群組內進行，他們正在制定憲章並縮小專案的目標和範圍。

四、核心數據模型與資料完整性：會議討論了有關各個規範進展的問題，包含核心數據模型、狀態列表、協作計劃。核心數據模型部分，討論了 VCDM 的進展情況。有一些問題需要在 CR（候選推薦）之前解決，但經過討論後，認為

有可能在 CR 之前解決這些問題。此外也討論了 VCJOSE-COSE 的進展，特別是添加 DID（去中心化識別）支持的問題。再來還有 VC 狀態列表的進展，指出在 TPAC 期間已經解決了一些重大問題，這將有助於後續的 PR（推薦）工作。

五、其他：GS1證書鏈用於識別貿易商品，講者介紹了新的 GS1證書鏈案例。該案例聚焦於 GS1識別系統，GS1是條碼標識的管理機構。該識別系統的核心是由 GS1管理，然後委派給世界各地的組織。該案例關注如何使用 GS1證書來識別貿易商品，以及如何處理併購情況。還提到了升級到 VC2.0數據模型以及關於證書狀態的考慮。

肆、心得與建議：

這次出訪行程是一個極具價值的經驗，疫情年之後，網路組織相關會議回歸實體，本次除了實際參與 TPAC2023，也和不同國家的民間企業組織、官方部門有所交流，就網路標準導入、網路發展史、次世代網路標準制定等有深入討論。臺灣作為 W3C 正式成員，能夠實際參與國際組織標準制定是難得的事情，此外根據 W3C 的行事風格，強調組織內的「個人」以其自主意願參與不同工作組進行協作，而非被其所屬組織所綁定。因此活躍積極的個人，可以為 W3C 帶來飛躍性的貢獻，並為其所屬組織帶來正面影響力，這對於全球網路事務而言，都是非常正面的回報。

近10年來，W3C 的標準建議已經逐漸從網際網路的軟體協定層面，擴散至文化經濟層面。軟體協定層面與瀏覽器重度綁定，這是因為現代網路使用者的使用媒介以個人電腦或行動裝置之瀏覽器為主，對於一般使用者而言，上網不太容易繞過瀏覽器，因此許多軟體協定的工作組，不同瀏覽器的開發者具有相當的發言權，如 Chromium、Firefox、Edge 等等，以上現象可見於與網頁超文字應用技術工作小組（Web Hypertext Application Technology Working Group, WHATWG）與文件物件模型（Document Object Model, DOM）協作之 HTML 工作組為首；而文化經濟層部分，更進入次世代網路基礎建設之必要元素，如強調個人身份自主權的可信賴憑證、分散式身分、聯邦宇宙（Fediverse 或於 W3C 內稱為 ActivityPub）、社會關聯式資料協定（Solid Protocol）等。後者工作組與相關標準文件如雨後春筍般成立，更進一步引入多樣化的參與者加入 W3C 組織。對於數位部民主網絡司而言，這些協定的精神舉措正好與我們此刻正在研擬之數位公共建設相同，若可早一步對齊國際標準，便能在網路技術層次先行與不同政府、企業、非營利組織與開放原始碼組織互通交流。最終使全民受惠。

此刻網路治理的世界有許多國際組織肩負標準制定的工作，如網際網路工程任務組（Internet Engineering Task Force, IETF）、網際網路名稱與數位位址分配機構（Internet Corporation for Assigned Names and Numbers, ICANN）、歐洲電信標準協會（European Telecommunications Standards Institute, ETSI）...等等，W3C 也正面臨標準競逐的時代。多方關係人組織所制定之標準如何為終端使用者所使用，有賴網路各階層的服務供應商與公共服務組織所使用，此間包含國家主權

層次的數位貿易談判、跨境商業平台自律與技術導入、非營利團體倡議與國內廠商的配合等等。綜上所述，以上多方關係人牽涉到實質權力與技術演進的模式，數位發展部肩負全民參與與全民數位福祉等任務，在標準開發的過程，為臺灣此刻與未來的網路使用者發聲，是理所當然的目標。因此參與國際民主網絡事務，可以縮短臺灣數位網絡環境落後的狀態，跟上國際腳步。

根據以上現狀，提出對於臺灣之於 W3C 可持續深化的參與形式建議如下：

一、促進部內各單位參與工作組，跟上時代脈絡：持續處理整合型業務，如諮詢委員會之代理事務等，維護臺灣身分與持續參與實效；此外也積極成為數位部業管繁體中文使用區之翻譯領導組織（Lead Translation Organization, LTO），將各式標準文件導入臺灣；並促進部內與相關組織成員實際參與各工作組，持續定期於內部交流實體進度；最後為將相關標準納入數位公共建設的工作項目，讓臺灣數位環境的基礎建設在第一步便創造可互通性，進行跨境資料交換。以數位公建相關組織為例，可積極參與的工作組分為身份與資料交換層，如社會關聯式資料協定社群組（SolidCG，目前正在成立工作組）、聯邦式身份社群組（Federated Identity Community Group, FedID CG）、前述分散式身分識別符、可信賴憑證等、關於平台身分互通的 ActivityPub 協定、隱私工作組與 AI 道德相關組別等。

二、積極與產官學研社橫向交流與推廣標準導入：目前臺灣民間企業尚缺乏透過標準制定或相關專利獲利的模式，因此民間較少積極參與網路標準組織。臺灣的網路環境尚以官方制定，民間跟隨的方式進行，相關案例如網頁內容可及性規範。而業界參與有賴技術專家參與，專家目前仍多服務於國際型數位服務提供之廠家，因此仍以大型跨境平台為主。解決方法可以以數位部名義舉辦技術行研討會，以相對低門檻方式引入有興趣的業界人士參與。

三、以翻譯案牽動多方關係人初步參與：官方與非官方的合作翻譯專案，可以有效接軌繁體中文使用區，尤其是臺灣的多方關係人。以最近在執行的網頁內容可及性規範2.1版本（WCAG2.1）官方翻譯為例，數位政府司以委外翻譯完成2.1版本，民主網絡司透過「行政院身心障礙者權益推動小組」委員名單邀請與招募具有意願的組織，共有十數間國際與國內組織有興趣參與中文校對等工作。可見官方翻譯過程可以輕巧有效地促進民間與產業參與國際事務。適逢網頁內容可及性規範2.2版本（WCAG2.2）版本於2023年十月發佈，以及本司正

在執行的分散式身分識別符標準，明年可望繼續加大翻譯力度與規模，聯繫上更多臺灣的網路標準開發人士，產生公私協力之效果。

四、重構部內合作形式，並有效匯集民間力量：如何以部內身分廣邀技術專家進行協作，仍是待解議題。目前的 W3C 部內積極參與者為國家資通安全研究院的兩位總顧問為主，這是因為這兩位成員已經有長期 W3C 協作經驗，如何順利延續顧問的經驗，也是我們必須嚴肅看待的議題。

伍、附件：

一、TPAC 回國報告簡報分享

概要

1. W3C & TPAC 簡介
2. W3C 的國際地位
3. 網路的本質
4. W3C 本身的治理
5. W3C 的隱憂
6. 與數位公建可能連結的工作組簡介
7. W3C 台灣的參與形式
8. 數位部參與再定位
9. 建議路線圖

形式

全球資訊網協會（W3C）是一個國際多利益相關者社群，由成員組織、全職員工和群眾共同合作，開發開放的網路標準。

影響

W3C制定的HTML和CSS標準是網站建設的基礎技術。此外還提供了支撐現代企業在娛樂、通訊、數位出版和金融服務等領域的標準。

轉型

W3C 於1994年由網路發明者Tim Berners-Lee創立，目標為促進一致的架構，以適應網路標準的進展。W3C於2023年重新啟動，形成獨立組織。

規範

W3C的規範是在公開的環境中創建的，根據W3C專利政策免費提供，並滿足公民社會在可及性、國際化、安全性和隱私方面的需求。

形式

TPAC 由 TP 與 AC 組成，分別為技術大會與諮詢委員會。TPAC 集結 W3C 成員和董事會、W3C 工作組和興趣組，來協調解決技術問題與治理進度

影響

在TPAC期間，WG和IG聚集在一起，進行交流並解決網路面臨的技術或社會問題，是W3C協調跨組織技術問題的重要手段。且多數記錄是公開的

本次參與

1. AC: D2
2. TP: D3
3. WG, IG, CG: D1, D2, D4, D5

網路的本質

(非瀏覽器)

經濟
文化層

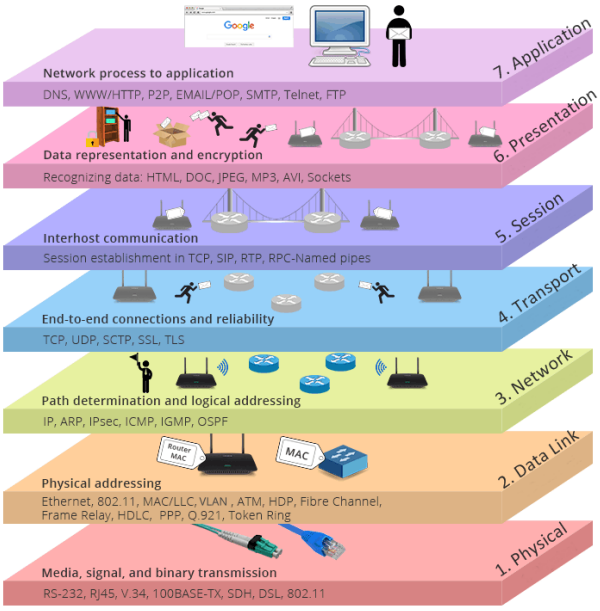
(瀏覽器)

軟體層

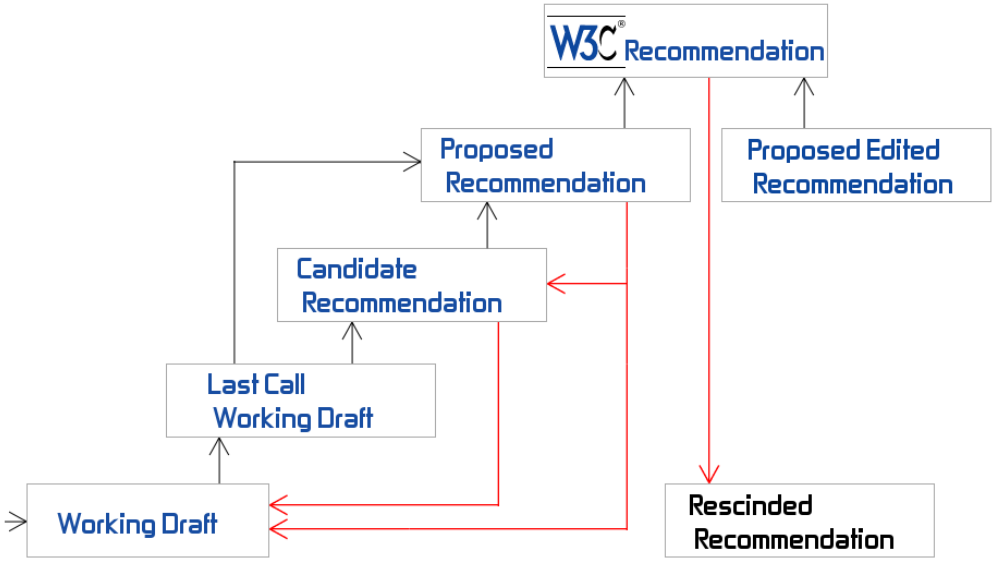
硬體層

W3C

DIDs, VCs, SOLID, ActivityPub 等等



W3C 本身的治理



W3C 本身的治理

2. **W3C Evaluation of LTO Submission**:

   W3C對LTO提交的評估：

   1. W3C acknowledges the LTO's submission of intent to develop an Authorized Translation. W3C may stop the process at this point, either because it does not consider the submission to be acceptable (see, for example, additional note 'g'), or because it does not consider the required effort to be justified in terms of the general operations of W3C. In general W3C will *not* approve multiple authorized translations for the same document and language, although issues such as French vs. Canadian French, or Portuguese vs. Brazilian Portuguese will be considered on a case-by-case basis.

      W3C承認LTO提交了開發授權翻譯的意向。W3C可能會在這一點上停止進程，要麼是因為它不認為提交是可接受的（例如，參見附加註釋'g'），要麼是因為它不認為所需的努力在W3C的一般運作中合理。通常情況下，W3C不會批准同一文件和語言的多個授權翻譯，但法語和加拿大法語，葡萄牙語和巴西葡萄牙語等問題將根據具體情況進行考慮。

   2. If the submission is approved by W3C, W3C notifies the LTO to proceed with the preparation of a Candidate Authorized Translation.

      如果W3C批准了提交的內容，W3C會通知LTO繼續準備候選授權翻譯。

3. **LTO Preparation of Candidate Authorized Translation (CAT).**

   準備候選授權翻譯（CAT）的LTO。

   1. The LTO prepares a Candidate Authorized Translation (CAT) of the document.

      LTO為該文件準備了候選授權翻譯（CAT）。

   2. When complete, the LTO announces the CAT and its URI on the translators' mailing list..

      當完成時，LTO會在翻譯者郵件列表上宣布CAT及其URI。

4. **W3C Initiation of Review Process**:

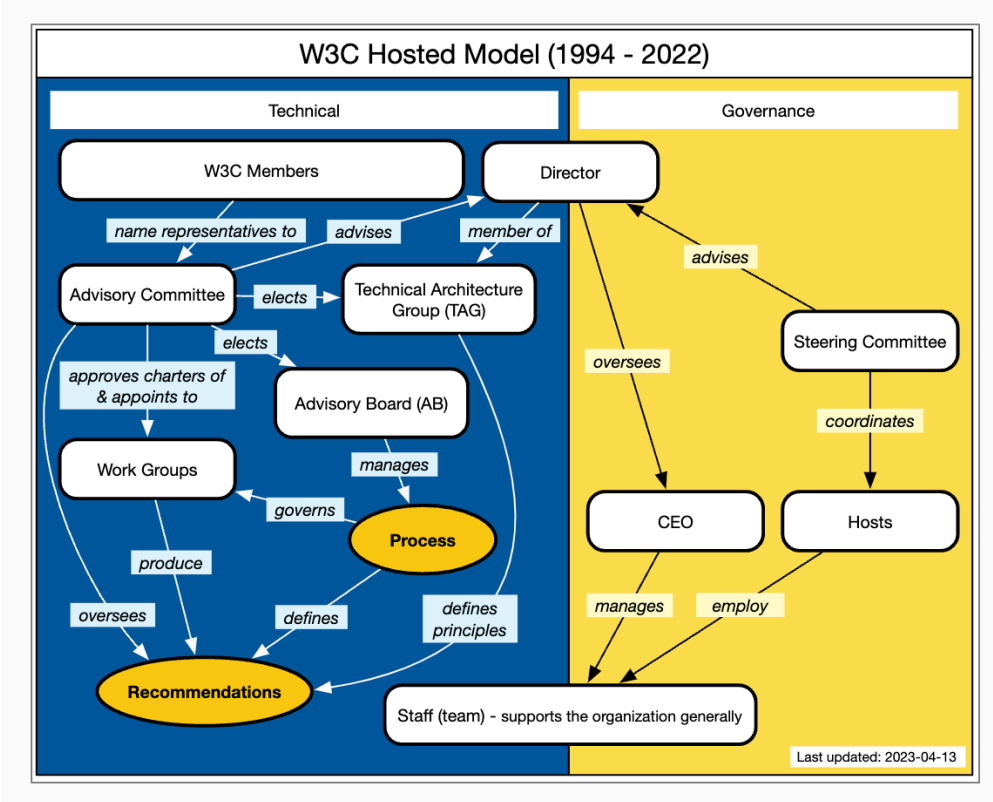
   W3C 審查程序的啟動：

   1. W3C announces a review period of at least 30 days of the CAT on the translators' mailing list, specifying a separate, publicly archived mailing list, in W3C or W3C Chapter Web space, to be used for commenting. This mailing list may be a per-language list for all CATs in that language, such as `public-auth-trans-hu@w3.org` for any Hungarian CAT, or a list specifically set up for that CAT. All comments on the CAT must be sent to this list. Postings to the mailing list may either be in the language of translation or in English.

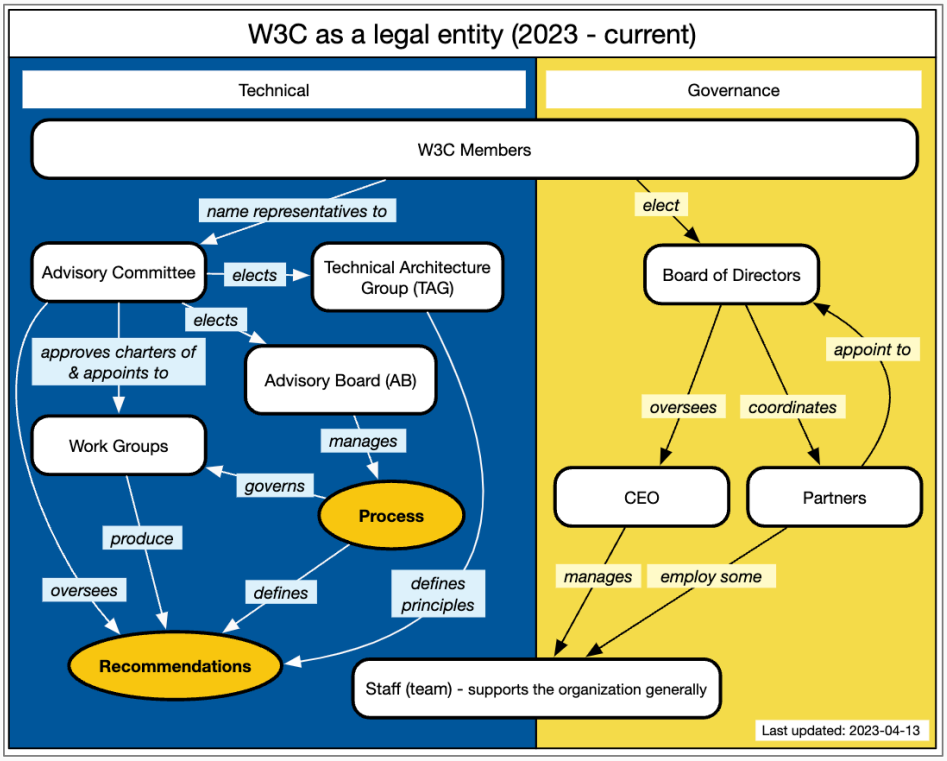
      W3C宣布在翻譯者郵件列表上進行CAT的審查期至少30天，並指定一個單獨的、公開存檔的郵件列表，該列表位於W3C或W3C Chapter網頁上，用於評論。這個郵件列表可以是每種語言的CAT的單獨列表，例如對於任何匈牙利語的CAT，或者是專門為該CAT設立的列表。所有對CAT的評論都必須發送到這個列表。郵件列表上的發帖可以使用翻譯語言或英語。

https://www.w3.org/2005/02/TranslationPolicy

W3C 本身的治理



W3C 本身的治理



W3C Process Document

12 June 2023

This version:
https://www.w3.org/2023/Process-20230612/

Latest published version:
https://www.w3.org/Consortium/Process/

Editor's Draft:
https://www.w3.org/Consortium/Process/Drafts/

Previous Versions:
https://www.w3.org/2021/Process-20211102/
https://www.w3.org/2020/Process-20200915/
https://www.w3.org/2019/Process-20190301/
https://www.w3.org/2018/Process-20180201/
https://www.w3.org/2017/Process-20170301/

Feedback:
Github (preferred)
Public mailing list
Member-only mailing list

Editors:
Elika J. Etemad / fantasai (Invited Expert)
Florian Rivoal (Invited Expert)

Former Editors:
Natasha Rooney (Invited Expert)
Charles McCathie Nevile (Yandex)
Ian Jacobs (W3C)

W3C的使命是制定促進其發展和確保可互通的共同協議，引領W3C發揮其全部潛力。W3C Process 描述了W3C的組織結構以及使其能夠完成使命的流程、責任和功能。

Vision for W3C

W3C Group Draft Note, 25 July 2023

▼More details about this document

This version:
https://www.w3.org/TR/2023/DNOTE-w3c-vision-20230725/

Latest published version:
https://www.w3.org/TR/w3c-vision/

Editor's Draft:
https://github.com/w3c/AB-public/tree/main/Vision

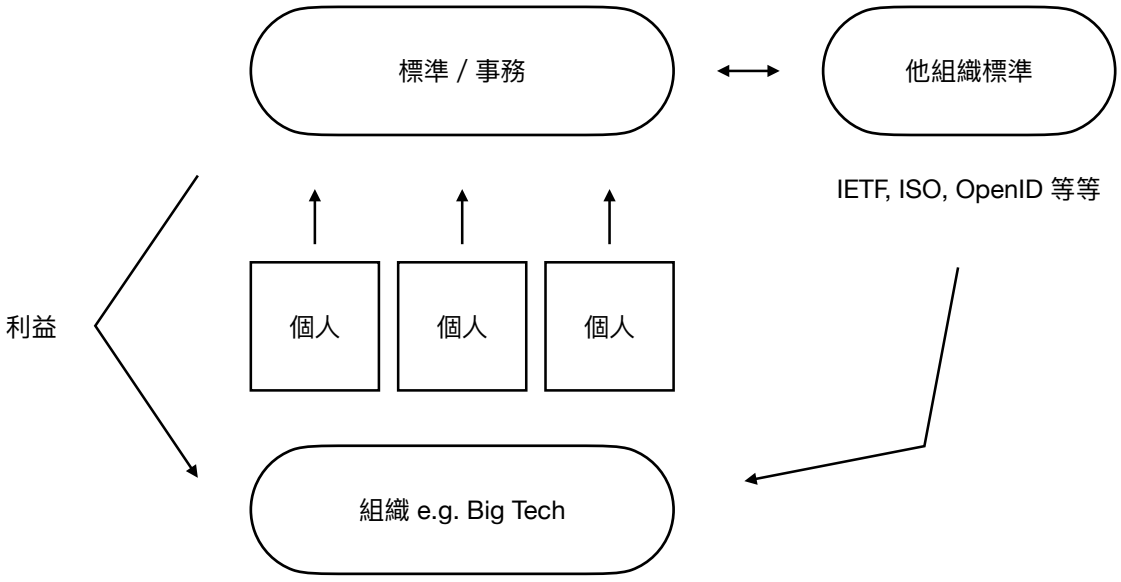
History:
https://www.w3.org/standards/history/w3c-vision/

Feedback:
GitHub

Editor:
Chris Wilson (Google)

這份文件是W3C的使命、價值觀、目的和原則的表達，換句話說，我們對於W3C作為一個組織在Web本身的願景中的定位。這個願景的目標不是預測未來，而是制定共同原則來指導我們的決策。**技術並不價值中立**，對特定技術的偏好或反對應該受到這裡所表達的價值觀的影響，但這個願景應該是思考這些事情的指南，而不是包含具體答案。

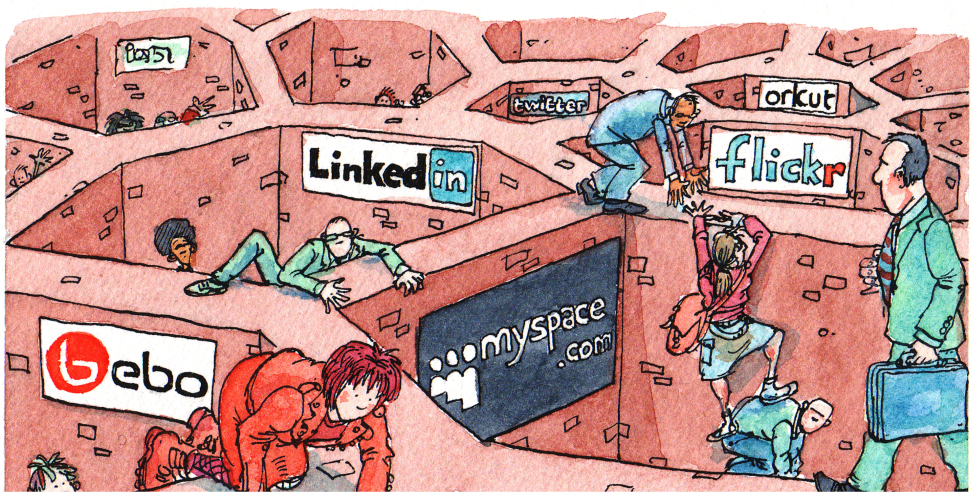
W3C隱憂：標準之間的競爭



Solid Protocol

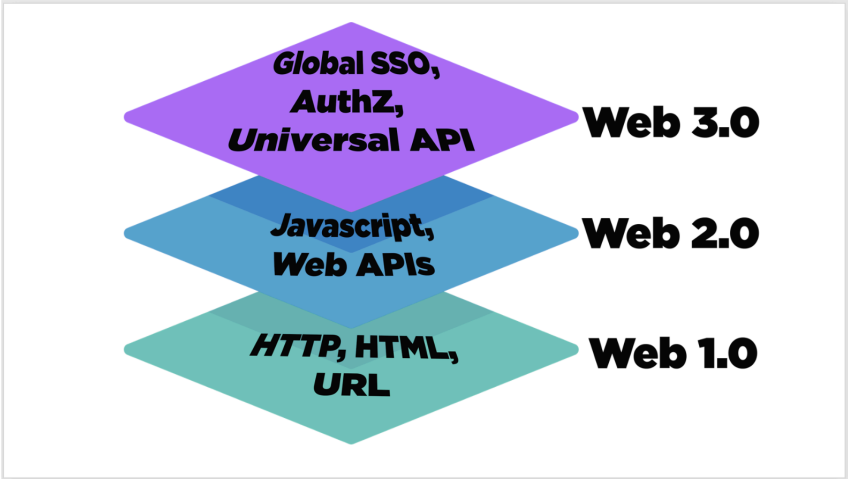
but ... data silos

are dis-empowering for individuals.



Web 3.0

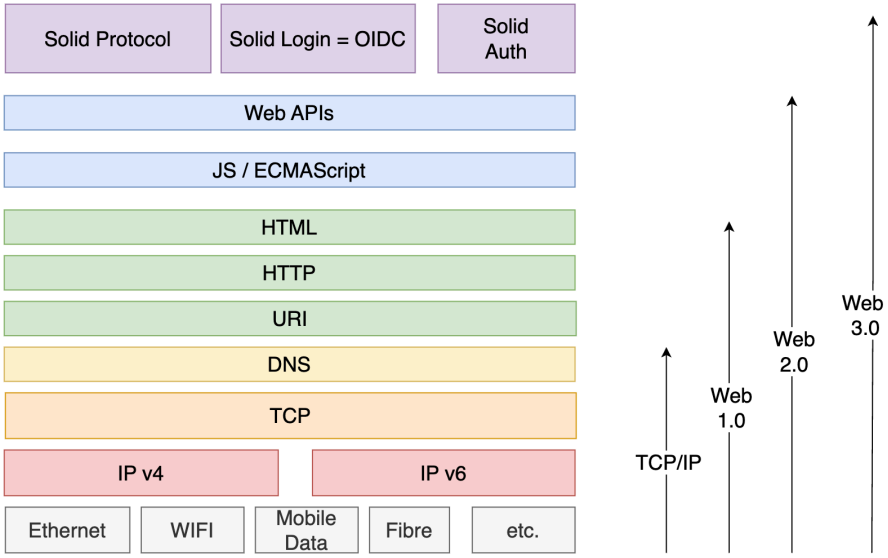
Now, to solve some of the problems of Web 2.0, there are new standards to give users control over their data.



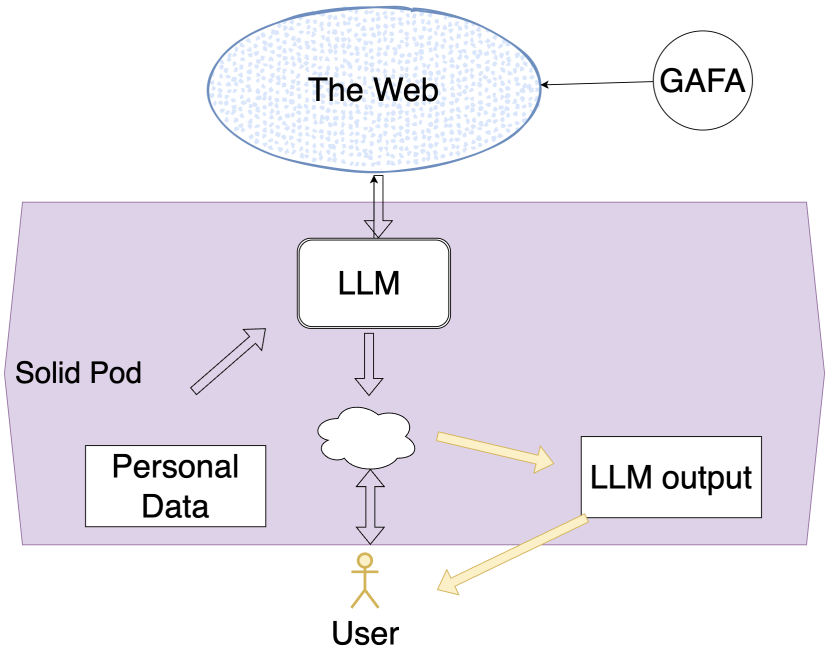
This has nothing to do with Blockchain!

Web 3.0

Single Sign In, and a common API so any App can store data in any Pod.



Imagine re-wiring



Ethical Principles for Web Machine Learning

W3C Group Draft Note, 11 August 2023

▼ **More details about this document**

This version:
https://www.w3.org/TR/2023/DNOTE-webmachinelearning-ethics-20230811/

Latest published version:
https://www.w3.org/TR/webmachinelearning-ethics/

Editor's Draft:
https://webmachinelearning.github.io/webmachinelearning-ethics/

Previous Versions:
https://www.w3.org/TR/2022/DNOTE-webmachinelearning-ethics-20221129/

History:
https://www.w3.org/standards/history/webmachinelearning-ethics/

Feedback:
GitHub

Editor:
Anssi Kostiainen (Intel Corporation)

Former Editor:
James Fletcher (BBC)

台灣民間的參與形式

1. 業界尚無標準制定者
2. 業界參與有賴專家
    1. 台灣的產業特質
        1. 標準的順應者
        2. 缺乏國際數位廠家
    2. 標準制定者具有紅利
        1. 數位標準與數位公共財
        2. Big Tech

數位部參與再定位

1. **國際參與**（積極參與W3C治理）
    1. Alter AC Rep.
2. **部內實質參與**（普及服務）
    司署的參與形式（時區問題、語言問題）
    1. 個人名義 vs. 公司名義
    2. 習於外包 vs. 實質協作
    3. 行政專業 vs. 技術專業
3. **技術專家**（專家參與各標準制定）
    1. 除了資安院顧問，應該如何加入？
    2. 部內是否有能力輸出貢獻回W3C?
4. **鼓勵外部參與**（產業標準互通）
    1. 翻譯（LTO 翻譯）
    2. 業界連結
    3. 2023 舉辦中大型研討會

日本做法：慶應大學、Big CO.、本土化優勢

W3C Communications with Members

1. Visit onsite
2. Have a call
3. Chat using social medias
4. Mailing list in Japanese (archive)
5. Japanese Member Meeting twice a year (sample: 2022/10/31's overview page)
6. Online study sessions on the 4th Tuesday of each month at 3:00pm
7. Inviting members to exhibit at the W3C booth at Interop Tokyo in June and Keio University's research event in November
8. Japan Executive Committee Forum
9. #jp on IRC for AC meetings

2019 spring Japanese Member meeting at Keio University

Interop Tokyo in 2018

W3C Web and W3C Promotion Activities in Japan

1. For technology to reach global standards
2. For the appeal of standardization in the country
3. Award system

結論：moda @W3C 下一步

1. 非官方翻譯
2. 官方翻譯
3. 國內研討會
4. 媒合本土 big player/標準制定型 NGO 實質參與
5. 盤點各國政府的參與形式