

出國報告（出國類別：開會）

全球資訊網協會年度大會 （W3C TPAC 2024）

服務機關/姓名職稱： 數位發展部 丁皓元 高級分析師

派赴國家/地區：美國/安那翰

出國期間：113年09月22日至113年09月27日

報告日期：113年11月22日

目錄

摘要.....	3
壹、簡介	4
貳、目的	6
參、過程	8
一、出國日期.....	8
二、出國行程.....	8
三、分散式識別符工作組相關會議重點.....	9
四、分組討論.....	31
五、W3C Plenary 與 W3C@30	35
肆、心得與建議.....	42

摘要

113年全球資訊網協會（World Wide Web Consortium，以下簡稱 W3C）年度大會於美國舉辦，這次會議邀集了許多來自全球各地的技術開發者、學者、商業機構、政府機關，分聚於各 W3C 工作組（working groups）和興趣組（interesting groups）進行發人深省的討論和協調工作，以解決全球資訊網所面臨具有挑戰性的技術和社會問題。

因本部於本（113）年度已正式啟動「數位皮夾」之公共建設，其發展初期即以 W3C 相關標準為基礎規劃整體數位皮夾，爰本次行程主要參加實際採用標準之分散式化識別符（Decentralized Identifiers, DID）工作組會議，了解最新的技術趨勢，並共同討論如何完善與精進 DID 標準、後續可能的應用合作與對接互通；亦於分組討論階段簡報我國數位皮夾發展推動規劃，分享發展經驗、特色及挑戰，並與來自不同產業及國家的專家進行交流，尋找潛在的合作機會，更展示我國對開放標準和網際網路發展的承諾。

W3C 為各網際網路標準領域與技術的重要國際組織，也是長期耕耘專業與建立夥伴關係的場域，本次與會於正式會議與會餘時間，進行跨國家組織聯繫與數位皮夾應用場景串聯，與來自多國的專家學者討論分享各國的數位政策、產業發展規劃並交流可能的合作機會，推動跨部門、跨領域的連結創新，期以數位發展成果行銷臺灣，增加我國能見度及國際交流。

壹、簡介

全球資訊網協會（World Wide Web Consortium, W3C）於83年在美國麻省理工學院（Massachusetts Institute of Technology, MIT）成立，由網際網路的發明者 Tim Berners-Lee 創辦。其主要目的是推動網際網路的標準化，以確保網路使用的可訪問性、互操作性和可持續發展。W3C 的願景是「讓每個人在任何地方都能自由地使用網路」，並促進網際網路的開放性與共享性。通過制定標準，W3C 致力於消除不同設備和平台之間的障礙，確保網站及網頁內容能夠被所有人輕鬆存取訪問。

截至113年，W3C 於4個主要地區的合作夥伴分別為：美國麻省理工學院、歐洲資訊與數學研究聯盟（European Research Consortium for Informatics and Mathematics, ERCIM）、日本慶應義塾（Keio）大學及中國北京航空航天大學。此外，W3C 擁有超過450個會員，包括大型企業、新創公司、學術機構和政府機關等，其中也有許多知名科技公司，如微軟、Google、蘋果、亞馬遜和 IBM 等，還有許多開放源碼組織和非營利機構，這些會員在推動網路技術的發展中扮演著重要角色；會員亦橫跨多個產業，包括科技、電信、金融、教育、醫療和媒體等，跨領域多樣性使得 W3C 能夠涵蓋廣泛的需求和視角，制定出更具普世性的標準。

近期，W3C 在多個領域取得顯著進展。例如隨著 Web 3.0的發展，資料的互操作性和智能合約的實現成為可能，這為未來的網際網路帶來了新的機會與挑戰；而在無障礙網頁設計方面，W3C 推出了更嚴格的無障礙指導方針，進一步強化了對特別需求人士的輔助；W3C 也積極推進網頁性能優化和安全性標準的

制定，以大幅提升用戶的網路體驗和資訊安全。

本部自112年加入 W3C，今年為第二次參與一年一度的諮詢委員會與技術大會（Technical Plenary and Advisory Committee, TPAC），配合本部於今年開始推動「分散式驗證及授權系統（數位皮夾）」之數位創新關鍵基礎公共建設即採用 W3C 標準建置，後續本部將積極參與相關網際網路標準的制定過程，對未來技術發展提出意見及分享我國經驗，並由此獲得最新的標準資料、實驗工具和技術報告，進而提升數位皮夾本身技術能力與使用安全，同時與來自不同產業及國家的專家進行交流，尋找潛在的合作機會，並展示我國對開放標準和網際網路發展的承諾。

W3C 為各網際網路標準領域與技術的重要國際組織，亦是長期耕耘專業與建立夥伴關係的場域，透過此協會展現我國數位軟實力，並適時瞭解他國科技相關資訊，再配合我國現有國家政策及產業產品，規劃發展與各國及產業的合作，對內可在政策層面更好地預測未來的技術變革，制定具有前瞻性和可持續性的政策，對外則可進行實質的數位外交工作，參與全球數位政策的制訂，期有效建立我國數位科技的國際能見度，也能對國際數位外交議題合作相關事務發揮更大影響力。

貳、目的

- 一、參加全球資訊網協會年度大會（W3C TPAC 2024），瞭解 W3C 整體運作、技術發展重點、應用及推廣之國際趨勢及現況，並評估未來如何深化本部與 W3C 之合作可能。
- 二、參加與本部「數位皮夾」高度相關之分散式識別符（Decentralized Identifiers, DID）工作組，透過了解各國政府、產業界及學術界的前沿技術及架構發展現況，評估我國數位皮夾推動及規劃可能方向及可補強處，從而提升運作效率和公眾滿意度。未來亦可將我國實際導入政府部會與民間應用場景之相關建置經驗回饋國際標準工作組，以有利於我國實質參與國際標準制定與推行，強化我國公共建設與國際標準發展組織之交流來往，發揮國際影響力。
- 三、以「Digital Wallet Project in Taiwan」為題，就「公共程式」、「開放生態系」、「沙盒環境」及「技術諮詢委員會」等 4 個面向分享我國數位皮夾現況與未來想像，並與多國專家進行討論，持續完備及優化我國數位皮夾推動規劃，確保相關規劃的可持續性和靈活性，期為國內「數位皮夾」帶來國際技術交流機會，以發展符合國內產官學研社需求之營運模式、信任架構與驗證生態系。
- 四、於會議期間及正式會議之餘，進行跨國家組織聯繫，促進跨政府或跨國產業應用場景串聯，與多國（美國、義大利、新加坡、日本、韓國及其他國家）專家學者進行交流，說明我國推動數位皮夾之規劃及架構，並討論請益本部強化參與如 W3C 等數位國際組織之可能方式，進一步促進國際交流，

擴大我國公共建設之影響力，建立國際伙伴關係。



會議期間與多國專家、學者及政府官員討論，摘錄會談照片左上為新加坡政府科技局（Government Technology Agency, GovTech）Calvin Cheng 首席軟體工程師、右上為新加坡資訊、通訊及媒體發展管理局（Infocomm Media Development Authority, IMDA）Pei Sheng Isaac Koh 經理、左中為 W3C 邀請專家 Daniel Burnett、右中為日本慶應大學 Shigeya Suzuki（鈴木茂哉）教授、左下為台灣數位出版聯盟（W3C 另外一臺灣會員）葉文熙組長、費志偉

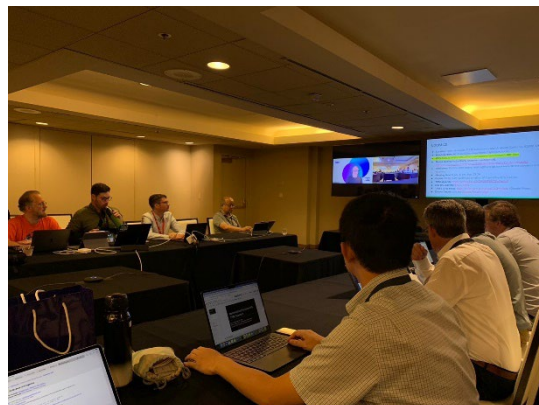
參、過程

一、出國日期

113年9月22日至113年9月27日。

二、出國行程

日期	行程
9/22（日）	臺灣桃園機場啟程及抵達美國洛杉磯／安那翰
9/23（一）	參加全球資訊網協會年度大會（DID 工作組）
9/24（二）	參加全球資訊網協會年度大會（DID 工作組）
9/25（三）	參加全球資訊網協會年度大會（分組討論、大會及30年慶祝活動）
9/26（四）	美國洛杉磯啟程
9/27（五）	抵達臺灣桃園機場



左圖為本次會場入口；右圖為 DID 工作組會場

三、分散式識別符工作組相關會議重點

W3C 為網際網路標準制定組織，由各工作組（Working Group）為主要執行單位，討論方式包含（依不同工作組而定）線上會議、實體會議（如 TPAC）、郵件列表（Mailing List）、GitHub Issues 及網際網路中繼聊天（Internet Relay Chat, IRC）等。有鑒於本（113）年度本部已正式啟動「數位皮夾」之公共建設，爰9月23日及24日參與之行程專注於實際採用標準之 DID 工作組會議，本次 DID 工作組有3位共同主席，主要由 W3C 邀請資深專家 Daniel Burnett 主導議程，並由 Will Abramson 與 Gabe Cohen 協同主持，相關會議討論內容摘述如下：

（一）DID 產業現況，講者：Gabe Cohen, Block, Inc.及 Manu Sporny, Digital Bazaar

本演講主要討論了 DID 當前狀態及其應用，並探討了多個正在使用 DID 的專案及其潛力。演講內容摘要如下：

1. 去中心化社群網路 Bluesky 採用 DID 標準，以 did:plc 方法實作建立可自認證、可復原、金鑰可輪替的機制，目前採用中心化的註冊表（registry），隨著用戶增長，將逐步提出更去中心化的 DID 方法。目前 Bluesky 上已註冊逾1000萬個 DID，未來潛力可達數億至數十億個 DID。
2. TruAge 為用來驗證年齡之機制，迄今約有數十萬用戶，將來約有4300萬潛在用戶，應用範圍擴展至便利商店等多領域。
3. 加州車輛管理局（California Department of Motor Vehicles，簡稱 CA

DMV) 使用 did:jwk (使用 JSON Web Key) 與 did:web, 當前有60萬個 DID, 每日約新增1200個, 潛在用戶數量為2700萬至3400萬。

4. 美國國土安全部 (US Department of Homeland Security, DHS) 使用 did:web 與 did:twid (Trust DID Web, 為 did:web 的延伸版本), 皆有數千萬潛在用戶。
5. Switchchord 使用 did:web 納入音樂創作者與發行公司之間的既有管理系統, 目前僅一個音樂出版商參與, 潛在用戶為1000萬以上的音樂創作者。
6. 歐盟區塊鏈服務基礎設施 EBSI (European Blockchain Services Infrastructure, EBSI) 使用 did:ebis 給法人、did:key 給自然人, 遵循 W3C 標準並符合 GDPR 規範, 約有4億4900萬以上的潛在用戶。
7. 不丹 (Bhutan) 國家身分系統使用 did:sov (由 Sovrin 基金會設立之 self-sovereign identity 解決方案)、Indicio Network 以及 Hyperledger Indy 區塊鏈, 約有79萬以上潛在用戶。
8. Velocity Network 使用 did:velocity 與 Velocity Distributed Ledger 來發行憑證, 並用 did:ion 與比特幣二層網路 ION 作為組織與個人的身分識別, 專注於職業紀錄及職業網絡, 當前有70多家公司, 已發出超過100萬份證書。
9. TBD 為 Block 公司 (前身為 Square) 部門之一, 專注於提供各種身分解決方案, 使用 did:dht (Distributed Hash Table, 為諸多 P2P 點對點傳輸協定所採用方案)、did:web 與 did:jwk, 專注於 KYC 和身分

認證，當前創建的 DID 超過300萬，包含 Square、Cash App 等產品用戶。

本場演講最後討論了 DID 目前面臨的一些挑戰，包括缺乏標準化的 DID 方法、一些歐盟成員對 DID 的抵制，以及對大型組織所需功能的不足等。這次演講強調了 DID 的實際應用及其潛力，展現了其在多個領域的應用範圍和未來發展的機遇，同時也反映出當前面臨的挑戰，呼籲各界在標準化和功能完善方面的進一步努力。

本演講簡報如下：

State of the Industry (30 min) — Manu, Gabe

10

Overview

- Decentralized Identifiers are in production!
- The following slides summarize:
 - How some of these projects are using DIDs,
 - The number of people using DIDs today,
 - The potential number of people using DIDs for each project.
- We will cover some upcoming events and challenges at the end

11


Bluesky

Details

- [did:plc](#) - Placeholder DID Method
- DID PLC is a self-authenticating DID which is strongly-consistent, recoverable, and allows for key rotation.
- Supports a permanent, publicly accessible history.
- Meant to be temporary until a better DID Method comes along. Run out of a centralized registry.

Today: Over 10,062,511 DIDs on Bluesky

Potential: Could grow to hundreds of millions to billions



12


TruAge

Details:

- [did:key](#) - Ephemeral key-based DID Method
- A simple, non-registry based DID Method based on expanding a cryptographic public key into a DID Document.
- Used to identify issuers and holders in the ecosystem.
- Convenience store sector: expanding usage of Verifiable Credentials (and DIDs) beyond age verification - coupons, loyalty, payments, digital receipts (potential to use [did:web](#) here)

Today: Several hundred thousand in [TruAge](#)

Potential: 200M+ in US at scale, with 52 million age checks per day



13


California Department of Motor Vehicles

Details

- [did:jwk](#) and [did:web](#)
- Used to identify CA DMV issuer and holder devices in Verifiable Credentials

Today: 600K with ~1.2K added per day

Potential: 27-34 million people in California with IDs through the State



14


US Department of Homeland Security (USCIS)

Details

- [did:web](#)* - [did:web](#) with [did:tdw](#)-like enhancements (e.g., DNSSEC)
- Used to identify DHS issuers

Today: Ready for deployment

Potential: 43 million permanent residents and naturalized citizens



15

Switchchord



Details:

- [did:web](#)
- Used to model legal relationships between music publishers and songwriters and route data about new music into existing catalog management systems.

Today: one music publisher with 10 songwriters; one publishing administrator that represents ~8,000 songwriters (current pilot is limited to 100); and ~100 independent songwriters.

Potential: 10M+ creator economy musicians, plus thousands of record labels and music publishers.

16

European Blockchain Services Infrastructure (EBSI)

Details:

- [did:key](#) extension (canonicalized JWK value)
- A W3C-compliant, privacy-preserving and GDPR-compliant did:key method.
- [did:ebsi](#) for Legal Entities; uses a permissioned blockchain network across Europe

Today: ???

Potential: 449 million+ people



17

Bhutan National Digital Identity (NDI)



Details:

- Launched in 2023 to create a national digital trust ecosystem in Bhutan
- Facilitates p2p interactions between individuals, governments, and organizations, accelerating digital adoption and access to financial and other services.¹
- Uses [did:gov](#), using the [Indicio Network](#) and [Hyperledger Indy](#) blockchain.

Today: ???

Potential: 790,000+ people

1. <https://trustoverdo.org/wp-content/uploads/Case-Study-Bhutan-NDI-National-Digital-Identity-ToIP-Digital-Trust-Ecosystems-V1.0-2024-05-21-en-it.pdf>

18

Velocity Network



Details:

- Focused on career records, and the Internet of Careers®
- [did:velocity](#) for credentials, uses the Velocity Distributed Ledger
- [did:ion](#) for organizations and individuals, a L2 that uses Bitcoin

Today: 70+ companies.¹ 1M+ credentials issued in 185 countries.²

Potential: Millions of workers, worldwide.

1. <https://www.velocitynetwork.foundation/foundation#general>
2. <https://www.velocitynetwork.foundation/velocitys-2023-recap-the-internet-of-careers-is-live>

19

TBD



Details:

- **TBD** is a business unit within Block (formerly Square)
- Focused on KYC, KYB, and providing identity for regulated financial use cases.
- Uses [did:dht](#), [did:web](#), and [did:jwk](#).

Today: DIDs created in the 3M+ range (mostly [did:dht](#)).

Potential: Millions of individuals and businesses using Square, Cash App, Afterpay and other Block products worldwide.

20

.... and more...



Privado ID: An EVM-based set of tools for developers to use W3C VCs and DIDs for use cases like age verification, national ID, content authenticity, and more. Uses [did:polygonid](#).



Dock: Customer onboarding acceleration with reusable ID. Uses a proprietary blockchain for [did:dock](#) (now merged with Cheqd).



Cheqd: Payment and trust infrastructure for credentials (now merged with Dock). Uses [did:cheqd](#), a Cosmos-blockchain based DID method.



Waltid: Digital identity and wallet infrastructure used by 10k+ developers and organizations. Supports [did:key](#), [did:jwk](#), [did:web](#), [did:cheqd](#).

21

.... many more!



Microsoft Entra: Supports [did:web](#) as part of the Entra Verified ID suite.



Trinsic: An identity acceptance network. Supports 16,000+ document types in 220+ countries. 20+ reusable ID schemes. 60M+ pre-verified users. Uses [did:key](#).



IOTA Identity Framework: Uses the [did:iota](#) method to facilitate a general purpose identity network for people, organizations, things, and objects.



GLEIF: Verifiable Legal Entity Identifiers powered by [did:webs](#). GLEIF has issued over 2.7M legal entity identifiers as of September 2024.

22

Challenges

- No *standardized* DID Methods (and governments need them)
- Pushback on DIDs by some in the European Union?
- [did:web](#) is lacking desired features for large organizations
- Even [did:plc](#) creators want something better
- People still want a *standardized* "decentralized" DID Method
- Will a DID Methods Charter get approval at W3C?

23

(二) DID 簡史，講者：Drummond Reed, W3C Invited Experts

此次討論的主題圍繞 DID 的演變及其當前狀態，D 講者說明

DID 一詞源自 Credential Community Group，同期關注此議題者集結成

群，於103年彙整為 DID 一詞。D 講者並強調了 DID 在數位身分控

制方面的重要性以及其去中心化特性，指出這一特性對於數位身分的安全性和隱私保護非常重要，並提到零知識證明等工具在保護用戶隱私中的重要性。

接著，美國國土安全部與其技術長資助了首份 DID 標準研發，旨在發展「永久有效的識別符、可解析、密碼學驗證、去中心化」此四種特性，其中 did:web 是最早發展出來的 DID 方法，規格與 URN（Universal Resource Name，定義於 RFC 8141）相仿。DID 方法始於32種，迄今已有198個方法註冊於 [w3c/did-extensions/methods](https://w3c.github.io/did-extensions/methods/) 裡，加上一些未註冊的方法，總計已超過200種 DID 方法。

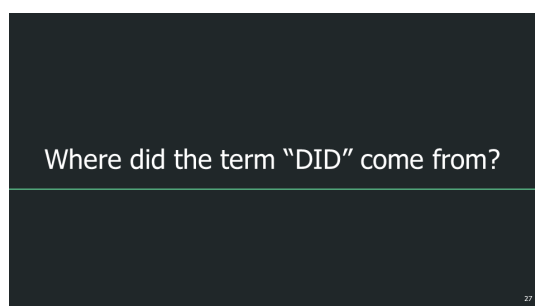
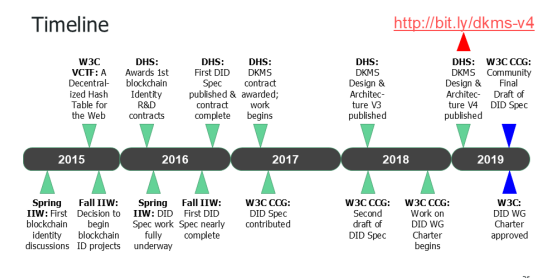
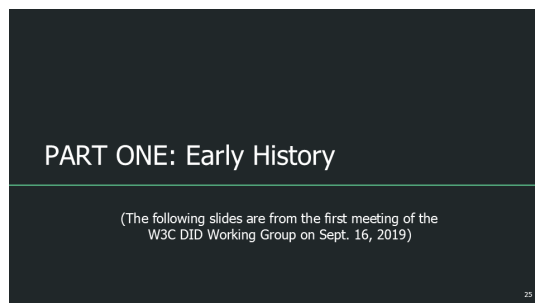
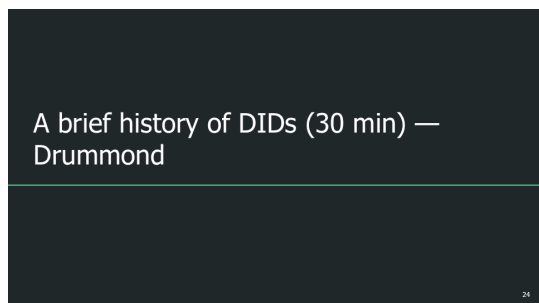
講者 Drummond Reed 曾於110年共同出版《Self-Sovereign Identity》一書（可於出版社 Manning 網頁上，免費閱覽全書內容），書中描述 DID 為數位控制中心（digital control point），由使用者裝置持有私鑰來持有控制權，相較於既有的電子郵件、手機號碼、網域名稱的控制中心則在於託管的伺服器。當時經常使用的詞彙是「分散式（distributed）」或「身分（identity）」，最終則決定為「decentralized identifiers（分散式識別符）」。

即使如此，本次工作組成員並非極端去中心化主義者，也能接受如 did:web 這種近乎中心化的方法，逐步讓去中心化方案變得可行，而非強制施行去中心化方案。

D 講者此次就 DID 的歷史、技術架構、去中心化的重要性及其未來方向進行了全面的探討，為與會者提供了豐富的見解和未來的發展方向，並鼓勵與會者進一步探索深入了解 DID 的演進及其在數位身分管理

中的應用可能。

本演講簡報如下：



A Decentralized Hashtable for the Web
Draft Community Group Report 03 April 2018

W3C Community Group Draft Report

Latest editor's draft:
<https://opencreds.org/specs/source/webdht/>

Editors:
Manu Sporny (Digital Bazaar, Inc.)
Dave Longley (Digital Bazaar, Inc.)

Authors:
Manu Sporny (Digital Bazaar, Inc.)
Dave Longley (Digital Bazaar, Inc.)

Version control:
Github Repository
Issues

Copyright © 2018 the Contributors to the A Decentralized Hashtable for the Web Specification, published by the Credentials Community Group under the W3C Community Contributor License Agreement (CLA). A human-readable summary is available.

§ 2. Terminology

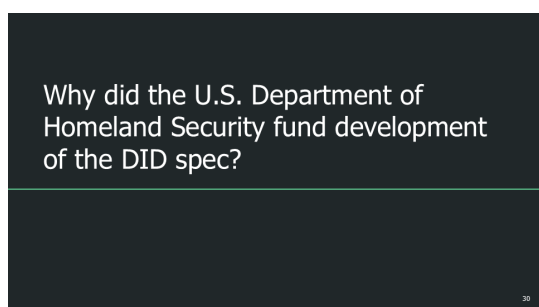
This document attempts to communicate the concepts outlined in the Open Credentials space by using specific terms to discuss particular concepts. This terminology is included below and linked to throughout the document to aid the reader:

credential
A set of claims that refer to a qualification, achievement, personal quality, aspect of an **identity** such as a name, government ID, preferred payment processor, home address, or university degree typically used to indicate suitability.

credential inspector
An **entity** that requests a **credential** for processing.

decentralized identifier
A portable URI-based identifier, also known as a DID, that is associated with an **entity**. These identifiers are most often used in a **credential** and are associated with **recipients** such that the **credential** itself can be easily ported from one **identity provider** to another without the need to reissue the **credential**. An example of a DID is: `did:b6922d8e-28df-4939-95cd-f79375979178`

decentralized identifier document
A document that is accessible via the WebDHT and contains information related to a particular **decentralized identifier** such as the associated **identity provider** and public key information.



Four reasons:

- 1. A permanent (persistent) identifier**
It never needs to change
- 1. A resolvable identifier**
You can look it up to discover metadata
- 1. A cryptographically-verifiable identifier**
You can prove control using cryptography
- 1. A decentralized identifier**
No centralized registration authority is required

What does a DID look like?

32

URNs (Uniform Resource Names, RFC 8141)

Scheme
urn:uuid:fe0cde11-59d2-4621-887f-23013499f905
Namespace Namespace Specific String

DIDs

Scheme
did:example:123456789abcdefghijk
DID Method DID Method Specific String

33

How widely are DIDs in use today?

34

Some statistics

- There are currently **32 DID methods** registered in the informal W3C Credentials Community Group DID Method Registry
 - <https://w3c-ccg.github.io/did-method-registry/>
 - Three for Bitcoin
 - Six for Ethereum
- The Sovrin Foundation currently has **71 stewards** around the world hosting a public permissioned distributed ledger for DIDs
- The Canadian provinces of British Columbia and Ontario have issued **over 1.4 million verifiable business license credentials** based on DIDs

35

For a full history, see:

<https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/topics-and-advance-readings/did-primer-extended.md>

36

PART TWO: A Quick Update

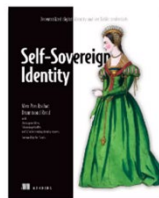
(The following slides are from an Evernym webinar given a few weeks after the W3C vote on DID 1.0)

37

Chapter 8: Decentralized Identifiers

"DIDs are the atomic building block of decentralized digital trust infrastructure."

<https://www.manning.com/books/self-sovereign-identity>



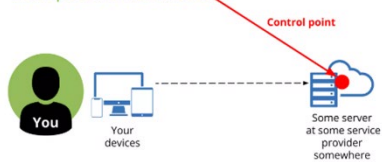
38

In simple terms:

A DID is a digital **control point**.

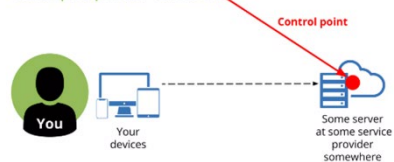
39

Example: email address

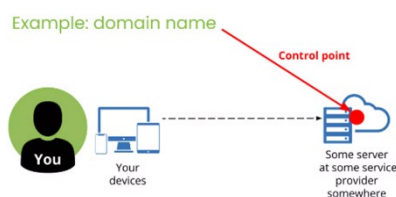


40

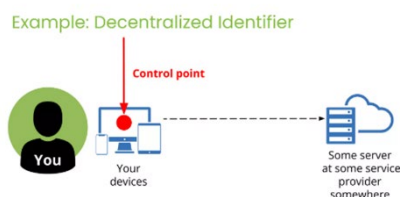
Example: phone number



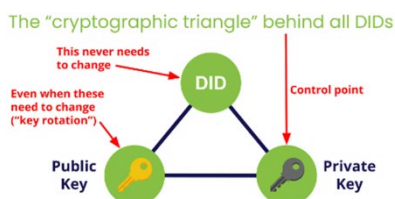
41



42



43



44

DIDs are the innovation that democratizes cryptography so that **everyone** can use it.

45

(三) DID 方法標準化，講者：Kim, Decentralized Identity Foundation

議程接著由「分散式識別符基金會（Decentralized Identity Foundation，以下簡稱 DIF）」的 Kim，介紹始於113年7月30日公開發表的一封合作意向信，由四個組織 DIF、Trust Over IP（ToIP）基金會、W3C Credentials Community Group、W3C DID 工作組，以及諸多相關成員共同連署，聲明將共同推動 DID 方法標準化，並將 DID 方法分為以下三個類別：

1. 可自解析（Self-resolvable）或單一金鑰（single key）方法，譬如 did:key 和 did:jwk。
2. 基於 Web 的方法，譬如 did:web 和 did:tdw。
3. 去中心化方法，譬如 did:dht。

預期將始於標準化幾個重要的 DID 方法，繼而將共同要求推廣

至不同類別，並將廣泛考慮方法成熟度、普及率、特質（traits）、測試向量（test vector）與至少兩個獨立實作之測試套件（test suit）。會議中討論了跨組織的可能合作方式，譬如 W3C 可專注於標準化基於 Web 的方法，意即 did:web 和 did:tdw。

（四）自我描述（Self-describing）的 DID 方法，講者：Kevin Dean, Legendary Requirements

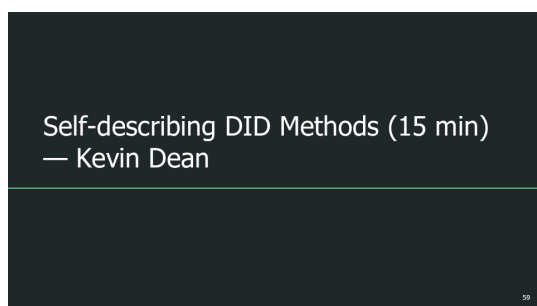
本演講說明過去基於「去中心化」的設計，並無規定方法名稱，亦無中心化的註冊機制，僅有軟性的「DID 方法註冊庫」（<https://github.com/w3c/did-extensions/tree/main/methods>），這使得「方法名稱衝突」與「版本控制」的管理極為困難。會議中討論了各種可能的做法，包含引入亂數與雜湊機制、如何確保方法名稱仍為人類可讀等。

K 講者一開始提到了 DID 方法未必唯一的問題，他指出，DID 方法缺乏版本控制可能會導致漏洞，因此建議在方法特定標識符中包含版本號，但目前尚未形成標準，且需要考慮主版本、次版本和補丁版本的關係，並建議在每個版本層級宣傳下一個可用版本的重要性。會中展示了版本控制的圖示，幫助理解不同版本之間的連接方式。

此外，K 講者進一步強調了生成 DID 方法名稱時，應以最小化衝突風險和確保安全的方式進行，他提出了幾種方法，包括隨機生

成固定長度字串、根據 RFC 9562 生成 UUID（建議使用第7版本）或將某個對 DID 方法使用者可訪問的文件進行雜湊處理，並建議方法名稱約定應便於人類可讀性。

本演講簡報如下：



The Problem

- DID method names are not guaranteed to be unique
 - Generated autonomously by the authors of their respective specifications.
 - May be mitigated by registering the method in DID Extensions (optional).
- Lack of version control
 - Vulnerability may require scrapping the DID method altogether.
 - No way to advertise a correlation between the previous DID method and the replacement DID method.
 - May be mitigated by including a version number in the method-specific identifier (not standardized).



Requirements

- Collision
 - DID method names SHALL be generated in such a way that there is a negligible risk of collision.
- Security
 - DID method names SHOULD be generated in such a way that they can be verified against some external, related content.
- Version Control
 - DID methods SHOULD advertise compatible DID methods that are usable without modification in processes involving the original DID method.
 - DID methods SHOULD advertise a replacement DID method that is an upgrade to the original DID method, not guaranteed to be usable without modification in processes involving the original DID method.



Semantic Versioning

- Versioning SHOULD align with the MAJOR.MINOR.PATCH concepts behind [Semantic Versioning 2.0.0](#), namely that:
 - incrementing the MAJOR version denotes incompatible API changes;
 - incrementing the MINOR version denotes functionality added in a backward-compatible manner; and
 - incrementing the PATCH version denotes bug fixes made in a backward-compatible manner.



Semantic Versioning

- A MAJOR.0.0 version SHALL advertise all its MAJOR.MINOR.0 (MINOR ≠ 0) versions as usable without modification.
- A MAJOR.MINOR.0 version (MINOR ≠ 0) SHALL advertise the next MAJOR.MINOR.0 (MINOR' = MINOR + 1) version as usable without modification.
- A MAJOR.MINOR.0 version SHALL advertise all its MAJOR.MINOR.PATCH (PATCH ≠ 0) versions as usable without modification.
- A MAJOR.MINOR.PATCH version (PATCH ≠ 0) SHALL advertise the next MAJOR.MINOR.PATCH' (PATCH' = PATCH + 1) version as usable without modification.
- All MAJOR.MINOR.PATCH versions SHALL advertise the next MAJOR'.0.0 (MAJOR' = MAJOR + 1) version as an upgrade, not guaranteed to be usable without modification.
- Any MAJOR.MINOR.PATCH MAY advertise any later MAJOR'.MINOR'.PATCH' (MINOR' = MINOR and PATCH' > PATCH or MINOR' > MINOR) version as usable without modification.



Semantic Versioning



Method Name Generation

- Names SHALL be set by some well-defined randomization algorithm (*[COLLISION](#)*). Some options are:
 - random fixed-length string generation using a cryptographically secure pseudorandom number generator;
 - UUID generation per RFC 9562 (version 7 recommended), minus hyphens; and
 - the hash of some document accessible to users of the DID method.
- The last option could be implemented as the hash of the DID method specification (*[SECURITY](#)*).
 - For the sake of this discussion, that option will be assumed.
- For future-proofing, the hash SHALL be represented using [multihash](#), encoded in lowercase [Base36](#) to minimize the method name length.



Version Advertisement

- There SHALL be a way to query a DID method, in a way that is accessible to all parties authorized to use the DID method, either in DID generation or in DID verification, for new versions of itself.
 - If there are restrictions around the use of a DID (e.g., access to the DID method's verifiable data registry requires presentation of some authorization token), those same restrictions MAY apply to querying the DID method.
- Three options for the DID method to provide this data are:
 - within the DID document data (assuming it is updatable);
 - within the DID document metadata (assuming it is updatable); or
 - via a service associated with the DID.
- The mutable nature of the version data better aligns with the concept of a service.
 - The "Version" (proposed) service type can be included in every DID document for the method, allowing the query to take place using any DID for the DID method.



Implementation

- Because the method name is the hash of the method specification, it's not possible to include the method name in the specification itself.
- Instead, the specification SHALL include the following statement:
 - The method name for this specification is the *<hash algorithm name>* hash of this document, represented using [multihash](#), encoded in lowercase [Base36](#).
- For the DID representing the DID method to be known, the specification MAY include the following statement:
 - The DID representing the DID method for this specification is `did:method-name:<method-specific-id>`.
- Depending on the algorithm for generating the method-specific ID, it may not be possible to know it at the time that the specification is finalized, so it may instead be shared through some out-of-band mechanism.



Standardization

- The preferred option is to update the DID standard to support self-describing DID methods.
 - [Class 4](#) change, hence out of scope of the current charter.
- The alternative is to register a new DID method (e.g., "x"), to support self-describing DID methods as sub-methods. This would include registration of the additional attributes and the "Version" service type.



Example

- Bitcoin-based DID method:
 - The method name for this specification is the SHA-256 hash of this document, represented using [multihash](#), encoded in lowercase [Base36](#).
 - The DID representing the DID method for this specification is `did:method-name:bc1qsvqcrsqhzm5frn45j1sctsfm7yeg38dvn9v2`.
- Once finalized, the hash is calculated and the final DID for the method is determined to be `did:mugx0x81mmlu9m5ysvjr222spgz8aovnrqbc063z2uutdzwtwsu:bc1qsvqcrsqhzm5frn45j1sctsfm7yeg38dvn9v2`.
- Method name and DID are published to the (private or public) community, with DID document including a "Version" service endpoint.



Scenarios

- See document for details.
 - DID Method Development
 - Patch Version
 - DID Creation
 - Minor Version
 - Minor Version Presentation
 - Major Version
 - Major Version Presentation



Questions?

Kevin Dean

kevin@legreq.com

<https://github.com/legreq/self-describing-did-methods>



71

(五) DID DHT，講者：Gabe Cohen, Block

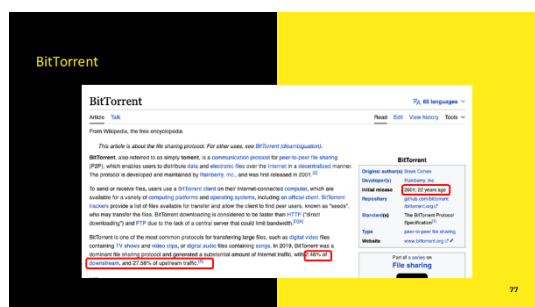
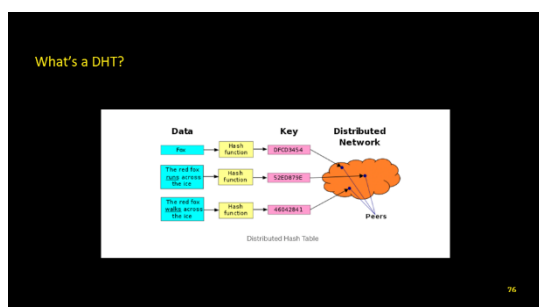
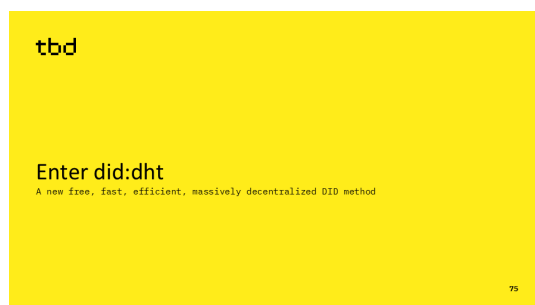
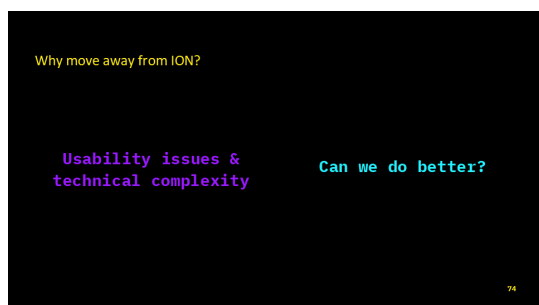
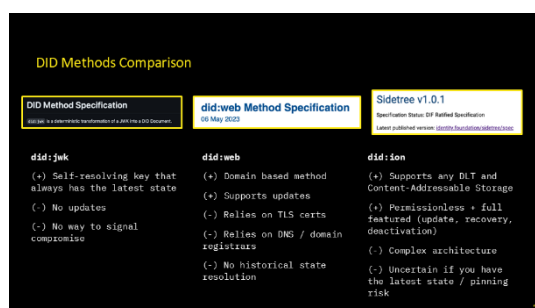
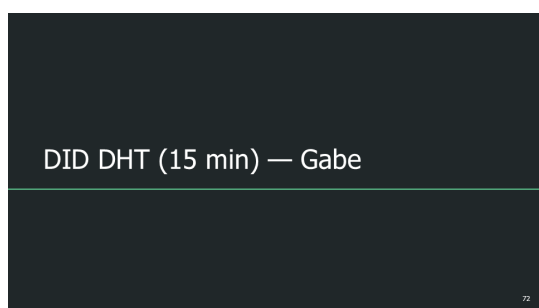
本演講主要介紹 did:dht（意指：<https://github.com/w3c/did-extensions/blob/main/methods/dht.json>），其基於比特幣區塊鏈的交易紀錄，回顧其發展限制（譬如：無法離線進行），並舉出幾種可能的解決方案供討論。

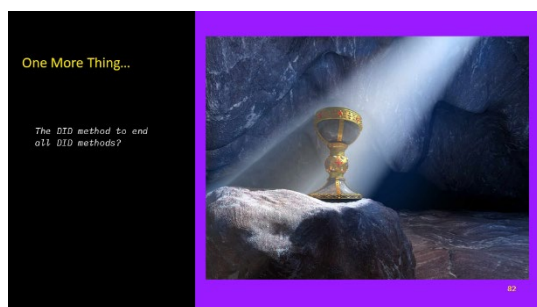
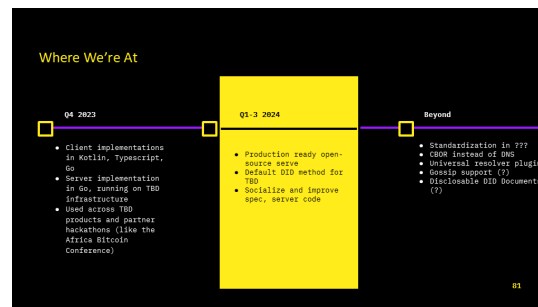
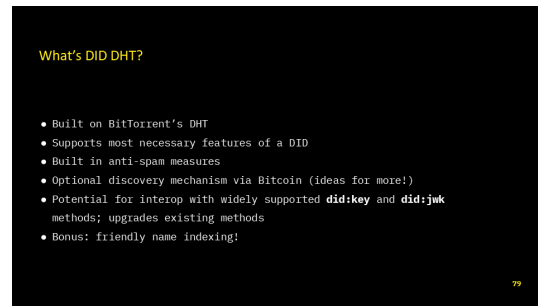
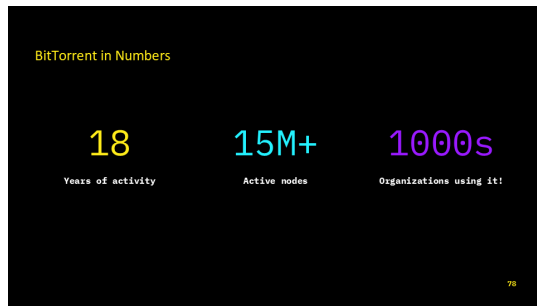
會議開始時，G 講者介紹了 DID DHT 方法的動機，指出其創建是為了解決包括發布延遲和低效的去中心化資料可用性。DID DHT 使用 BitTorrent DHT（Distributed Hash Table）作為穩健的解決方案，

擁有1600萬至2800萬個節點，並有超過1000個組織使用，其並支援大多數 DID 所需的功能，且內建反垃圾郵件功能。

G 講者接著也說明了 DID DHT 所面臨的挑戰，包括儲存效率和量子計算對安全的潛在影響，G 講者最後也提到，開源客戶端和伺服器的開發對 DID DHT 的成功非常重要，並希望將其標準化以提高效率。

本演講簡報如下：





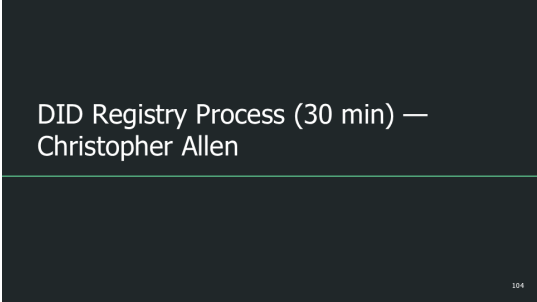
(六) BTCR 的經驗教訓和改進，講者：Joe Andrieu, Legendary Requirements

本演講主要介紹 `did:btc` (<https://github.com/w3c/did-extensions/blob/main/methods/btc.json>)，其源自 BitTorrent 的 DHT，採用 Ed25519 金鑰格式，並將轉向更有效率的 CBOR (Concise Binary Object Representation，為 IETF RFC 8949 格式)，迄今已建立超過 300 萬個 DID。會議中討論了 Ed25519 不具抗量子計算的未來風險，並預期會是未來探索的重點。

(七) DID 註冊流程，講者：Christopher Allen, W3C Invited Experts

C 講者首先說明了 DID 註冊流程的討論重點在於避免名稱衝突和去中心化的挑戰。目前已有198種方法註冊，但存在一些如包含過時的聯絡資訊和所有權變更等問題。C 講者強調，現行註冊過程需要符合可接受的方法規範，並有必要審查道德性或商標，以確保註冊的有效性。此外，C 講者接著提出可考慮使用 W3C 的註冊流程以確保名稱唯一性的要求，並建議設立一個為期1.5年的臨時註冊期，期滿後需延長期限或刪除相關項目，以有效解決目前問題。

本演講簡報如下：

 <p>DID Registry Process (30 min) — Christopher Allen</p> <p>104</p>	<h3>Some History</h3> <ul style="list-style-type: none">• Tension going back to RWOT2 (2016) between:<ul style="list-style-type: none">◦ Need to avoid name collisions◦ Risk of centralization of decentralization• W3C DID 1.0 Consensus<ul style="list-style-type: none">◦ First come, first serve; minimal requirements◦ Delegated to to W3C CCG during interim <p>105</p>
<h3>Current Method Registry</h3> <ul style="list-style-type: none">• Key requirement is a link to acceptable method spec• But also review of IP and moral issue of name• Currently 198 methods registered• CCG has new (trained early 2024) team reviewing registrations, no backlog• There are a number of problematic entries with no approved process to fix<ul style="list-style-type: none">◦ Contact no longer available◦ Ownership change◦ Some method specs no longer available◦ Version change◦ Desire to expire <p>106</p>	<h3>DID WG 1.1</h3> <ul style="list-style-type: none">• We agreed to split out the current DID method registry from other DID extensions.• Our charter requires we "Establish a deterministic mapping between DID method identifiers and the resolution process used to resolve that DID method."• As a WG, we can also now do official W3C registries.• We don't have consensus on processes to resolve current method registration difficulties• There also is some desire to:<ul style="list-style-type: none">◦ Have the list be shorter◦ Be able to differentiate registered methods <p>107</p>
<h3>One proposal</h3> <ul style="list-style-type: none">• We continue to have the CCG volunteers maintain the base "method registry",<ul style="list-style-type: none">◦ Primary goal to avoid name collisions◦ Continue with minimal spec requirements.◦ Have some simple policies to address current problems• These will be considered "provisional" for period (1-½ years?)<ul style="list-style-type: none">◦ A new PR each period can renew "provisional" for another period, otherwise removed.• That the DID 1.1 WG maintain additional lists, possibly including:<ul style="list-style-type: none">◦ Some proof of implementation in code and any deployment status◦ Conformance to the DID Resolution test suite◦ Supports some minimal web-based API• These additional lists are not W3C registries, more like Notes, and are not required to "be" a DID. <p>108</p>	

（八）DID Traits，講者：Dmitri Zagidulin, W3C Invited Experts

本演講討論了 DID Traits (<https://identity.foundation/did-traits/>) 的概念，由 DIF 維護，旨在為 DID 方法標記各種功能特質，譬如：是否支援 API 服務端點、金鑰輪替、可撤銷等機制，並進一步以常見的 did:key、did:web、did:tdw、did:dht 為例。會議中討論了 traits 的定義與定位，可能視為 DID 方法的「標示」，或更適合改稱為「功能 (features)」或「特徵 (characteristics)」，並強調具體、可重複使用的特徵比抽象模式更為重要。初步結論為可先將既有註冊的 DID 方法加上較無爭議的相關標示，譬如 immutable（意指 DID 文件更新是否儲存於不可篡改的資料結構，譬如分散式帳本）。

本演講簡報如下：

DID Traits, Feature Sets (30 min) — Dmitri

128

What are DID traits?

"LEGOs for DID method authors" (Design patterns of DID method construction)

Part of rubrics (technical affordances)

Example traits:

- Immutable vs mutable
- Support for service endpoints
- Support for alsoKnownAs
- Self-certifying identifiers
- Key rotation event logs / history
- Pre-rotation
- DID relative URLs
- Revocable / deletable
- Is the DID method signed?

129

did:key traits

Deterministic

Immutable

Offline capable

No support for: service endpoints, alsoKnownAs, history. more than one key

130

did:web traits

Mutable, revocable, deletable

Support for many key types, multiple keys

No key rotation history

Not self certifying

- Supports **alsoKnownAs**
- Supports **controller** property
- Service endpoints,

131

did:tdw traits

- Mutable, revocable, deletable
- **Self certifying identifier**
- Key rotation history log
- Pre-rotation
- /whois
- Supports **alsoKnownAs**
- Supports **controller** property

132

did:dht traits

- Mutable, revocable, deletable
- Updates through non-rotatable identity key pair
- Multiple keys, multiple key types
- Supports **alsoKnownAs**
- Supports **controller** property
- Supports service endpoints

133

See also

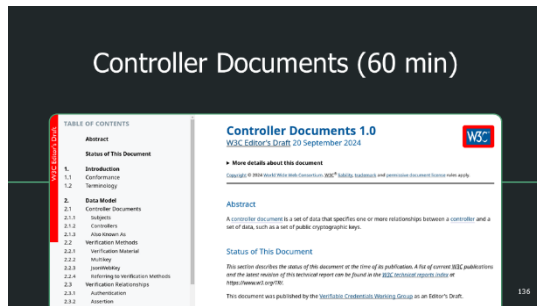
<https://identity.foundation/did-traits/>

134

（九）DID 控制者文件，講者：Manu Sporny, Digital Bazaar

M 講者接著討論了 Controller Document（控制者文件），說明該文件最初作為完整性規範的一部分進行開發，並希望避免對 DID 核心文件的直接引用。控制者文件的內容隨著時間演進，拓展至支援任何 URL 的普遍用途，演講中討論了其與 DID 文件的異同與維護性問題，包含應對 W3C 的 TAG（Technical Architecture Group）和 PING（Privacy Interest Group）的審核意見，儘管審核建議提出了一些擔憂，但這並未阻止文件的進展，目前係由 VC 工作組負責，文件即將邁向 Candidate Recommendation 階段，未來可能考慮轉移給 DID 工作組。

本演講簡報如下：



What is a "Controller Document"?

- A generalized type of DID Document that allows for ANY URL to be used in the document.
- The "class" that DID Documents inherit from.
- Current plan is to make the DID Core specification depend on the Controller Document specification.

... the plan is on track, more-or-less, with some weirdness

- VCWG is responsible for the Controller Document (due to Process issues, we weren't chartered at the time)
- Controller Document exists mainly because a few people didn't want to normatively reference DID Core or Data Integrity
- We were supposed to directly copy text from DID Core, but have ended up modifying it slightly

What's in the Controller Document today?

- Same properties as in DID Core: id, controller, alsoKnownAs, verification relationships and methods
- New-ish stuff:
 - Normative JsonWebKey and Multikey definitions
 - Multibase definition and base-encoding/decoding
 - Algorithms for fetching keys and base-encoding/decoding
 - JSON-LD Contexts that don't depend on DIDs

What is the timeline?

- Need to respond to TAG and PING review comments
- Pretty much ready for 1st Candidate Recommendation
- Expect 1st Candidate Recommendation in Nov-Dec 2024

Discussion

- **service** isn't in controller document, should it be?
- **service** isn't in VCDM, should it be (in v2.1 or v3.0)?
- Do we want to request transfer of Controller Document to this group?
- Are there any concerns about the current path?

(十) What's Interoperability? How can we test/demonstrate it, 講者：Dmitri Zagidulin, W3C Invited Experts

本場演講由 D 講者說明 DID 的互操作性挑戰及測試策略，互操作性範圍可分為於單一 DID 方法的互操作性（應意指不同實作）或跨不同 DID 方法間的互操作性。單一 DID 方法或可透過註冊時的自動化或解析測試機制來確保互通性，惟須注意各項規格細節，譬如：金鑰格式、API 服務端點支援度、自定義欄位等。此外，多數發行者、驗證者、與皮夾都僅支援部分的 DID 方法，使得跨不同方法變

得困難，譬如發證者可能會想要定期輪替金鑰，這就使得部分 DID 方法無法支援。DID 方法註冊與解析可採用自動化測試，但實際應用場景的互操作性測試並不容易。

會議中回顧了 DID 1.0 工作組章程中，僅處理資料模型與其測試套件，接著 1.1 工作組章程才到 DID Resolution（解析）與 API 互操作性。會議中繼續提出「功能性測試」應該直接視為「解析測試」（意即僅測試 DID 解析功能是否正常，而非直接測試整體功能是否正常），並強調自動化測試套件對 DID 解析和註冊的重要性，特別是在測試金鑰類型、服務端點和自定義屬性方面，D 講者亦將其視為下一步努力的方向。

本演講簡報如下：

<p>What's Interoperability? How can we test/demonstrate it? (30 min) — Dmitri</p> <p>142</p>	<p>What is interoperability?</p> <ul style="list-style-type: none">• What's in a DID?<ul style="list-style-type: none">◦ 1) bag of keys◦ 2) bag of service endpoints◦ 3) alsoKnownAs◦ 4) (possibly) controller hierarchy• Interop within a DID method vs interop between DID methods <p>143</p>
<p>who is concerned with interop?</p> <p>What is a DID used <i>for</i>?</p> <ol style="list-style-type: none">1. Signing stuff (authn, VCs, etc)2. Encryption/decryption3. Routing4. Aliases (alsoKnownAs) <p>144</p>	<p>Interop between DID methods</p> <p>First and foremost, interop on the policy level</p> <p>That is does a given system (issuer, verifier, agent) even <i>intend</i> to support a given DID method?</p> <p>Currently, most deployed issuers, verifiers, and wallets support a small curated subset of DID methods.</p> <p>Why? Affordances, tech constraints, library support, governance, policy, level of confidence</p> <p>145</p>

Interop within a DID method

- Registration testing (where applicable)
- Resolution testing

Watch for:

- Key type support
- Which service endpoints are allowed
- Are custom properties allowed?
- Infrastructure complexity (authentication, gas fees, etc)

146

Practical Interop Concerns

For a given DID method, how many registrar and resolver libraries in various languages?

For signing (e.g. VC issuance), do issuers and verifiers support a given set of DID methods? (interop through wide usage)

Similar question for authn (RPs), encryption, routing.

DID interop basically tied to the use case.

147

Bonus: DID based signature validation concerns

(beyond key type support)

Which Issuer and Verifier Registries support this DID method?

What about historical verification? (key rotation events, observers, logs, anchoring in time)

148

(十一) Extensibility of DID Resolution and DID URL Dereferencing，講者：

Markus Sabadello, Danube Tech GmbH

M 講者首先討論了解析 DID 的語法及功能，說明解析規範需具備的靈活性，並提供 DID URL 的解析範例，討論主要與次要資源及當前規範的術語，以及說明如何傳遞額外訊息至解析函數的問題，並對解析選項的一致性提出質疑，他提到為了解決解析器執行過多工作的擔憂，應該保持介面的簡單性。此外，現存的 URL Dereferencing 機制有許多模糊性，譬如參數可能放在 URL 的 path 或 queries 裡，但可能指向相同資源或者完全不同的功能。會議中討論了相關規格細節，尤其是釐清了 URL fragment 僅由客戶端解析。

本演講簡報如下：

Extensibility of DID Resolution and DID URL Dereferencing (30 min) — Markus

153

Resolving DIDs

```
did = "did:" method-name ":" method-specific-id
resolve(did, resolutionOptions) →
« didResolutionMetadata, didDocument, didDocumentMetadata »
```

154

Dereferencing DID URLs

```

did-url = did path-abempty [ "?" query ] [ "#" fragment ]

dereference(didUrl, dereferenceOptions) →
« dereferencingMetadata, contentStream, contentMetadata »

```

155

Examples of DID URLs

```

did:example:123456789abcdefghi#key-1
did:example:123?versionTime=2021-05-10T17:00:00Z
did:example:123?transformKey=JacoWebKey
did:example:123?noCache=true
did:tdr:Qmafmc1gDw38gwK6S85GQzF4.example.com#whole
did:tdr:Qmafmc1gDw38gwK6S85GQzF4.example.com/whole
did:tdr:Qmafmc1gDw38gwK6S85GQzF4.example.com/whole#vcl
did:tdr:Qmafmc1gDw38gwK6S85GQzF4.example.com/governance/issuers.json
did:chgtf:mainnet:46e2af9a?resourceName=degrees&resourceType=250MSchema
did:example:123?service=DecentralizedWebNode&query=W3gT0V

```

156

Where is it specified?

DID URL Dereferencer Functionality	Where is it specified?
Method-independent functionality	
<code>method</code>	DID_Spec and DID_Resolution
<code>key</code>	DID_Spec and DID_Resolution
<code>toolCaster</code>	DID_Resolution
<code>toolAssessable</code>	DID_Resolution Extension
Method-dependent functionality	
<code>resolutionTime</code>	DID_Spec and DID_Resolution and DID_Method_Spec(s)
<code>resolutionName</code>	DID_Resolution Extension and DID_Method_Spec(s)
<code>tools</code>	DID_Method_Spec(s)
<code>/whole</code>	DID_Method_Spec(s)
<code>/governance/issuers.json</code>	DID_Method_Spec(s)
Application Functionality	
<code>issuers</code>	Application-Spec

157

（十二） 共同討論：DID 測試套件/解析器測試套件

本節會議主要討論了目前及未來的 DID 測試套件狀態，現有的測試套件主要檢查 DID 的語法，涵蓋102種方法及約100個測試案例，但缺乏交互功能。與會者認為需要一個更全面的測試套件，不僅應包括解析和引用功能，還應可自動化產生測試報告（譬如既有函式庫的完整實作程度。目前需經 canivc.com 主動加入測試報告）。

會中也討論了測試套件是否應成為註冊 DID 方法前的必備條件（大部分與會者同意將測試套件的通過作為 DID 方法註冊的一部分，

可提高測試的有效性和權威性，並能有效降低審核編輯的人工負荷)，以及討論在 W3C 角色分工中，應由工作組負責將測試套件正式批准。

(十三) CBOR / CBOR-LD，講者：Christopher Allen, W3C Invited Experts

C 講者接著討論 CBOR 與 CBOR-LD 格式，是由 IETF 訂下的二進位表現格式，能執行語意壓縮，並在會議簡報上展示其資料格式效率，遠高於既有的 JSON-LD（但有些發言者指出，在某些情況下，對 CBOR-LD 進行 gzip 壓縮可能會導致文件大小反而增加），並可能藉此擴展應用場景至嵌入式系統，與會者同時確認了如 cbor-ld.js 等資源的存在，並支持保留多種 CBOR-LD 選項，以適應不同的使用案例。

本演講簡報如下：

CBOR / CBOR-LD Representation (30 min)

167

A CBOR-based DID Document

- CBOR Advantages
 - Binary, Concise, Self-Describing, Constrained Environments, Platform/Language Independent, Standardized (IETF), Deterministic (with CDE draft or dCBOR draft), compression (various drafts: cbor-packed, cbor-ld, gordian envelope)
- Disadvantages
 - Is not, by-default a triple-store (needs tag registration)
 - For JSON-LD-based DID Documents, i.e. **Self-Describing ≠ Context**

168

What's required of this group?

- Charter has "Plain CBOR Representation" as an "Other Deliverable"
- Existing Work
 - Plain CBOR Representation v1.0 (wg note 2021) <https://www.w3.org/TR/did-cbor-representation/>
 - Problematic, based on IPFS cbor tag, no deployment
 - CBOR-LD 1.0 <https://json-ld.github.io/cbor-ld-spec/>
 - Deployed; specific to linked data

169

DID Documents as CBOR-LD

CBOR-LD performs "semantic compression" on any JSON-LD Document.

```
graph LR; A[JSON-LD] --> B[Build Compression Dictionary]; B --> C[Compress]; C --> D[CBOR-LD]
```

A DID Document can be a JSON-LD document, making this transformation automatic and round-trippable.

170

符的使用上；而對於組織識別符，則不應使用中心化。會議強調在提出解決方案之前，應首先明確去中心化的問題，並建議以網路和 DNS 的去中心化回應反對去中心化的觀點。經與會者共同討論，工作組一致同意創建一份去中心化簡介，並將其整合到 W3C 的核心規範中。

四、分組討論

9月25日白天主要行程為分組討論，由各參與單位自由提出欲分享及討論之議題，當日白天除分別參加「探索義大利數位皮夾」及「在歐洲獨立實施數位皮夾的經驗及挑戰」等議程外，亦發表「臺灣數位皮夾專案」，相關分享討論摘要如下：

（一） 參與議程：Discover the Italian Digital Identity Wallet

義大利數位皮夾旨在讓民眾可以安全地使用數位化的公共和私有服務，並整合歐洲健康和殘障卡。該系統強調信任、安全和隱私，且使用 OpenID 技術提供唯一識別符，皮夾透過法律和技術規則提供身分證明、聲譽、安全和隱私的保障，並建立信任網絡以作為系統基礎。

在信任模型方面，義大利專注於可擴展性，致力於降低官僚成本，建立可擴展的信任框架，強調全球範圍內的信任能力。使用 OpenID 技術，參與者可透過 HTTPS URL 進行唯一識別，信任鏈的建立則利用第三方信任模型，並通過 JWT 標頭嵌入信任信息，允許

離線流程。

憑證的發行過程使用傳統數位身分系統（如 Spid ID）以強調安全性，也探討了使用一次性展示密鑰和零知識證明技術的可能性。義大利還制定了資料可攜性策略，要求用戶連線驗證以導入憑證備份，並強調實施所需的標準和技術參考的重要性。未來將開發憑證 API，重點在於安全性、隱私和信任框架，並尋求技術夥伴的合作，以填補與現行標準的差距。

討論中還涉及信任模型的可擴展性及先進技術的應用，義大利分享該國數位皮夾在小規模的驗證階段時，信任清單尚可控，但一旦大規模推動，信任清單的管控會非常困難。最後，演講者呼籲建立監管者與實施者之間的聯繫，強調用戶為中心的合作模式，期待未來的共同努力，以促進相關行業的發展。

（二）參與議程：Lessons learned by an independent implementation of the Digital Identity Wallet in Europe

本演講說明了在歐洲實施數位皮夾時出現的挑戰和困難，主講團隊基於歐盟數位身分技術架構框架文件（Europe Digital Identity Architecture and Reference Framework，簡稱 EUDI ARF），獨立實作了一套數位皮夾系統（該系統測試版展示可在 didroom 取得），並發布了所有程式碼免費開源，同時發現諸多議題，譬如：身分可被追蹤、撤銷機制未完備、要求手機的安全軟硬體皆需經認證、尚無考慮抗

量子計算、尚未建立完整的威脅模型等，另外也發現相關討論與人力皆缺少的資源問題。

**（三）發表議程：Digital Wallet Project in Taiwan，講者：數位發展部丁皓元
高級分析師**

本次演講主要分享了我國數位皮夾計畫，這是一個為期4年的專案，旨在建立一個可以確保數位身分安全，並便利日常數位生活的公共建設基礎設施。該計畫將創建一個數位身分框架，賦予用戶完全的控制權，確保最佳的隱私和可信的驗證，並將採用兩項 W3C 標準，包括分散式識別符（Decentralized Identifiers）和可驗證憑證（Verifiable Credentials），及利用身分自主權（Self-Sovereign Identity, SSI）框架，提供多項關鍵優勢。

此外，臺灣數位皮夾將採用開源模式，免費釋出數位皮夾 APP、發行者 SDK 和驗證者 SDK，讓全球所有政府機關和私營企業可以自由使用和修改軟體，無需事先批准，將可顯著加速驗證產業的進步和增長，並可同時確保臺灣的數位皮夾持續符合最新的國際憑證標準。

計畫還將建立一個沙盒環境，供前述組織測試他們的軟體和所需的驗證功能。這個沙盒環境允許開發者創新和創建新服務，而不會干擾線上實際運作環境，同時也讓網路安全專家提前檢查新功能以確保其安全性。

未來任何機構，包括政府和私營企業，都可以自由發行憑證和進行驗證，這促進了競爭的驗證產業，鼓勵安全可靠的驗證方法發展，也方便與國際夥伴的合作。

演講後聽眾主要關注議題（括號內為我方回應說明）在是否開放民間使用（是）、目標對象為何（民眾及員工）、是否跨國使用（是）、用哪種程式語言（Java）、是否與 EU 連結（標準互通）等，另中國出席人員亦於會後說明他們也在規劃類似東西，希望能與我們民間互通（我國跟隨 W3C 標準、注重人權及隱私並將開放成公共程式，歡迎他們可以參考我們的公共程式）等。

本演講簡報如下：

Digital Wallet Project in Taiwan
HaoYuan Ting,
Ministry of Digital Affairs,
Taiwan
TPAC 2024
Anaheim CA, USA
hybrid meeting
23-27 SEPTEMBER 2024

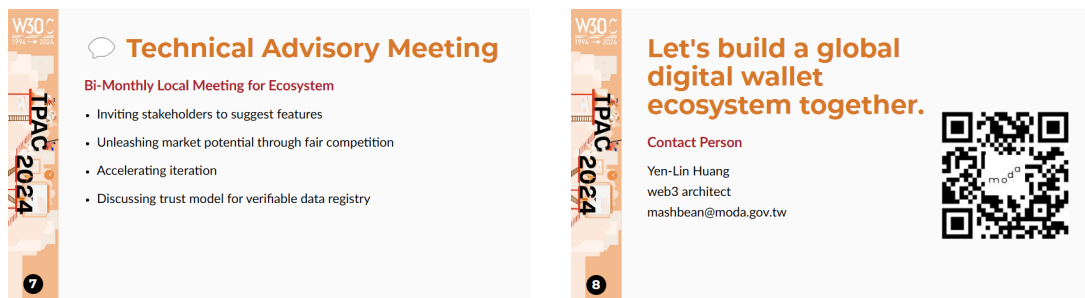
Digital Wallet Project
2024 - 2027
Build a universal infrastructure, securing digital identity with Self-Sovereign Identity (SSI) model.
Adopting W3C Standards
• Decentralized Identifiers v1.0
• Verifiable Credentials Data Model v1.1

Overview
• Public Money, Public Code
• Open Ecosystem
• Sandbox Environment
○ Technical Advisory Meeting

Public Money, Public Code
Open Source Software
• Unlocking Digital Wallet and SDKs for all
• Freely use and fork without prior approval
• Build a robust verification ecosystem together
• Aligned with latest verification trends

Open Ecosystem
For Issuer, Wallet, and Verifier
• Anyone can issue credentials, build a wallet, or conduct verifications without prior approval
• Foster competitive verification industry
• Facilitate international collaboration

Sandbox Environment
Playground for Innovation
• Testing features and functions
• Exploring ideas and creating new solutions
• Production environment unaffected
• Actively mitigate cyber risks



五、W3C Plenary 與 W3C@30

9月25日傍晚則為本次 TPAC 的 Advisory Committee Meeting，本年度會議型式為對所有會眾公開之 W3C Plenary，由 W3C 執行長發表演講，其中提及近年 Digital Identities 的重要性；而 W3C@30則為三十週年慶祝議程，由多位資深成員發表演講，演講重點摘要如下：

（一） W3C Plenary，講者： Seth Dobbs, W3C 總裁及執行長

S 講者本次的演講摘要涵蓋了多個主題，主要包括技術更新、財務狀況及團隊變動的進展。首先提及的內容是各個工作組和團隊近況的更新，主要討論了與網頁技術相關的重要議題，例如技術審查小組（TAG）正在持續進行設計審查，努力制定支持新技術開發的設計原則和文件，並發布了首個正式的網頁倫理原則聲明，以確保技術開發與其使命、願景和價值觀相一致。

S 講者接續提到隨著網路使用者人數的快速增長，網路的濫用問題愈加重要，例如防止使用者接觸到虛假資訊和不實資訊，確保使用者能夠辨別真實資訊。此外，數位身分的討論也成為焦點。數

位身分的發展正日益受到各國政府的關注，這可能會對網路和身分概念產生重大影響。

在隱私問題上，TAG 最近發布了關於 Cookies 的建議，強調了用戶隱私與用戶體驗之間的平衡。TAG 還發布了關於隱私原則的文件，以幫助開發者理解隱私的定義，並制定相應的設計原則。











在國際化（i18n）方面，雖然沒有重大新聞，但仍在為各類語言和文字提供支援。同時，WCAG 2.2標準正在向 ISO 提交，以讓更多國家能夠採用這一標準，並計畫在十月發布 WCAG2ICT 無障礙標準。


會議最後提到了一些財務狀況的更新，整體財務健康，會員費用增長超出預期，支出控制得當，並在感謝卸任團隊及歡迎新任團隊加入的掌聲中結束本場演講。

本演講簡報如下：

The image displays four slides from a presentation titled "2024 TPAC Plenary Session". Each slide features a vertical banner on the left with the W3C logo (1994-2024) and "TPAC 2024".

- Slide 1:** "2024 TPAC Plenary Session" by Seth Dobbs. It specifies the event is in Anaheim, CA, USA, a hybrid meeting from September 23-27, 2024.
- Slide 2:** "Agenda" listing three items: 1. W3C Technical Agenda Updates (Security & Privacy; Accessibility; Internationalization; APIs), 2. Corporate Updates (Finance; Team; Membership Survey), and 3. Board of Directors Election Results.
- Slide 3:** "TAG - Ethical Web Principles", described as "Underpinning the TAG's design principles and other technical work". It includes a link to "Ethical Web Principles".
- Slide 4:** "Security & Privacy", with the subtitle "Imperatives for a safe web".

	<p>"Society relies on the integrity of public information. We have a responsibility to build web technologies to counter misinformation and to maintain the integrity of information for public good. The public needs verifiable source and context information to recognize trustworthy web publishers and content."</p> <p><i>W3C Ethical Web Principles</i></p>		<h2>AI-driven risks & threats</h2> <p>AI can provide many benefits but is also bolstering security and privacy threats:</p> <ul style="list-style-type: none"> • Copyright threats • Misrepresentation / mis/disinformation • Deepfake • Rapid code generation could accelerate attacks, other misuses of the web
	<h2>Paths Forward</h2> <ul style="list-style-type: none"> • AI github discussion • C2PA and Content Credentials is one proposal put forth by the Linux Foundation Joint Development Foundation • Above builds on the work of W3Cs Text & Data Mining CG 		<h2>Digital Identities</h2> <p>Rapid increase in scope and scale</p>
	<h2>Identity Insights and Work</h2> <ul style="list-style-type: none"> • Identity and the Web • Digital Credentials - a draft community group report • FIWG Charter 		<h2>Identity - Safety & Privacy</h2> <ul style="list-style-type: none"> • User agent support of selective sharing • Viable for multiple stakeholders • Work in conjunction with other protocols and formats
	<h2>Identity and Privacy Challenges</h2> <p>Imagine a transaction with the government (needing a passport for clearing customs, or an identification to purchase liquor.)</p> <ul style="list-style-type: none"> • How does a user feel comfortable sharing information with the requestor? • How does the requestor trust the provided id? • How does the user ensure only the information needed is shared? 		<h2>Privacy - Moving forward</h2> <ul style="list-style-type: none"> • TAG recommendation on third-party cookies • Privacy Principles provides clarity on what we mean by privacy on the web
	<h2>Horizontal Updates</h2>		<h2>Accessibility Updates</h2> <ul style="list-style-type: none"> • WCAG 2.2 headed to ISO • Publishing WCAG2ICT in October • AI and Accessibility • Accessibility staffing




IPAC 2024

15

Advanced APIs

TAG continuing focus on advanced APIs across multiple implementor. Important and needed features should be developed with our principles in mind




IPAC 2024

16

Getting Involved

Interested in more on any of these subjects, please reach out to TAG and Team


TAG election coming soon!



IPAC 2024

17

Corporate Updates




IPAC 2024

18

Financial Update

- Growing surplus: revenue exceeding budget, expenses below budget
- Operating reserves: projected at 8.9 months
- Programmatic expense %: 75.0%
- Audit in process
- 2025 budget approved - relatively neutral




IPAC 2024

19

2024 Team Hires

- Simone Onofri (Security Lead)
- Ken Franqueiro (WAI Web Technical Specialist)
- Tamsin Ewing (Accessibility Content Specialist)
- Sylvia Cadena (Chief Development Officer)
- Tara Whalen (Privacy Lead)
- Tzviya Siegman (NA Member Relations, Sustainability Lead)
- Part Timers: Ken Troshinsky (CFO), Emma Fraser (Board Enablement)

Near completion of search for Director of Legal & Compliance




IPAC 2024

20

Membership Survey

We sent 824 emails and received 1200 results!

- 75% identified as male
- 50% describe themselves as developers or engineers, 40% in orgs with 10 or fewer employees
- 55% started W3C within last 10 years; 40% within last 4 years!
- 38% only participate in W3C; other organizations include ISO (23.9%), IETF (21.8%), WHATWG (18%), Unicode (15%)




IPAC 2024

21

Membership Perceptions


In general, most respondents felt we compared to other SDO's "about the same" in all areas (scoring 30-45%). However, our strongest areas (where the total of "Better" and "Much better" exceeds "about the same") were Openness, Fairness, Quality of Standards, and Overall perception.



IPAC 2024

22


Welcome to the new Board of Directors



IPAC 2024

23

Thank you outgoing Board of Directors



IPAC 2024

24

Thank You Team!

• Alex	• Marie-claire
• Amy	• Philippe
• Bert	• Gerald
• Vivien	• Denis
• Ralph	• Jean-Gui
• François	• Dom
• Ian	• Xueyuan
• Zhenjie	• Coralie

（二）W3C@30

1. One internet and the web，講者：Jun Murai,W3C,日本慶應大學教授

在 W3C 成立30周年的慶祝活動中，J 講者分享了個人與電腦科學的歷程，他回憶起19歲時讀到 Ted Nelson 的書《Computer Lib》和《Dream Machines》，提到 Nelson 在60年前提出的超文字（hypertext）概念，這為後來的 HTML 和網際網路奠定了基礎。J 講者指出，W3C 的標準化工作讓資料共用和網際網路的民主化成為可能，為每個人提供機會，對各領域造成深遠影響，並使得創造性和創新得以實現。

2. The web as a bridge across borders，講者：Fuqiao Xue,W3C Internationalization Lead

在慶祝 W3C 30周年的活動中，F 講者表達了對網路成就的感激和興奮，強調網路超越地理和文化界限的潛力。他回顧了 Tim Berners-Lee 最初設想網際網路作為知識共用工具，指出這一技術如何演變為連接數十億人的全球現象。

F 講者特別提到網路對教育的變革，偏遠地區的學生能夠訪問世界一流的資源，並與來自不同大洲的同伴進行虛擬課堂學習，這種知識的民主化使得歷史上被邊緣化的個體得以被賦權（empower）。通過網路，一位生活在偏遠地區的女孩能夠學習程式撰寫技能，並與數千英里外的導師和夥伴建立聯繫。

他還討論了這種連接的影響，網路使全球各地的人們能夠分享自己的故事和創新。來自非洲小村莊的藝術家可以向北美觀眾展示作品，南美的科學家可以與東亞的同行即時合作，這種互動促進了理解和共同的人類體驗。

儘管網路具有連接的力量，但 F 講者也指出我們面臨的挑戰，如資訊落差。他強調 W3C 在創建公平數位環境中的重要性，特別是在無障礙、國際化、隱私和安全等方面的標準制定。展望未來，F 講者呼籲進一步推動網路的包容性，確保其服務於所有人，無論語言、文化或能力。

3. Web & the art of specification maintenance，講者：François Daoust, W3C Media Specialist

在 W3C 30周年的慶祝活動中，F 講者討論了網路作為資訊基礎設施的重要性。他指出，網路已經成為人類日常生活中不可或缺的一部分，類似於電力和交通等基礎設施，而為了確保這些基礎設施的可持續性和韌性，我們需要不斷關注和維護網路。

F 講者強調，韌性是指系統適應意外事件的能力，網路必須具備這種能力，以便在下一個60周年慶典上繼續存在。F講者指出，W3C 在促進網路社群的鬆散協調方面發揮著關鍵作用，確保了各方在開放環境中的合作。他也對未來30年 W3C 能否繼續保持這種中心力量表示樂觀，並對所有為提升網路韌性而努力的人表示感

謝。

4. Supporting human rights in Web standards，講者：Nick Doty, Senior Technologist, Center for Democracy & Technology

N 講者在 W3C 成立30周年慶典上強調了網路在人權方面的重要性。他代表民主與技術中心，指出該組織自90年代以來一直參與 W3C 的標準化工作，並承諾繼續推動人權和網路標準的結合。

N 講者提到，《世界人權宣言》對網路的影響，強調了言論自由、集會和接受公共服務等權利的重要性。他認為網路已經成為人們進行政治組織、社交和獲取資訊的核心平臺，而 W3C 在推動這些權利方面發揮了關鍵作用。

同時，N 講者指出網路也面臨著監控、隱私侵犯、審查和安全等威脅，因此在標準工作中必須更加注重保護用戶和社會的責任。他呼籲網路技術的設計應優先考慮人權，確保這些權利在資訊世界中得到維護。

N 講者最後對 W3C 在推動倫理網路原則、隱私保護、無障礙設計等方面的努力表示自豪，並強調未來需要繼續擴大參與範圍，以更好地應對全球人權挑戰。慶祝成就的同時，必須牢記對社會的責任，積極推動網路技術與人權的融合。

肆、心得與建議

一、本部刻正推動的數位皮夾係屬新興數位工具，涉及多方合作，包括政府機關及其他各產業均可加入。為使各使用者及利害關係人使用之系統均可順利對接，發展初期本部即以 W3C 相關標準為基礎規劃整體數位皮夾，以提供跨部門、跨產業甚至跨國的對接，進而推動公共服務的資訊化轉型，強化政府提供數位服務的效能。

本次實質參與標準制定會議，繼而熟悉且協同討論相關議題，理解國際標準互通之重要方向，形塑工作組成員之間的討論互信。今年度著重參與的 DID 工作組討論，其內容比較偏技術面及操作面（如 method 的命名及管理方式、registry 的處理方式、控制者文件要包含什麼項目等），主要發言者約6-7人，雖多數參與者目前似較缺乏大規模實作經驗，但仍積極想要在標準制定上留下一筆；經觀察，如果明年我國數位皮夾有了初步成果，其實作發展經驗定可引起許多迴響。後續本部將持續參與標準制定之線上會議，並適時雙向反映對本部「數位皮夾」建置規格之影響評估，期可有效推動數位皮夾的標準化，確保與不同系統甚至不同國家間的互操作性。此外，因數位皮夾涉及多方、多領域合作，為確保數位皮夾在資訊安全、隱私保護、交易處理等方面遵循統一的國際技術標準，以提升數位皮夾的安全性，還能保證於後續推廣時，不被技術壁壘所困，爰未來將評估參與 W3C 其他業務組包含：

- （一）Threat Modeling Community Group：本社群組由 W3C 資安主管 Simone Onofri 成立，旨在推進 Threat Modeling 相關文件與討論。

(二) Verifiable Credentials for Education Task Force：本社群組由 DID 工作組邀請專家 Dmitri Zagidulin 擔任共同主席，旨在推廣教育證書（亦為我國數位皮夾規劃可能包含標的之一）。

(三) Credential Community Group：憑證社群組可視為 DID 與 VC 工作組（均為我國數位皮夾規劃之重要參考）的前身，亦持續與兩個工作組一起合作。

二、本次實體參與 TPAC 過程中，持續透過正式會議與會餘時間，進行跨國家組織聯繫與數位皮夾應用場景串聯機會。本次重要聯繫摘要整理如下，將跟進維持聯繫或討論可能的合作機會：

(一) Shigeya Suzuki 教授為日本 Trusted Web 重要成員，亦為本部數位皮夾已初步訪談之對象，未來將繼續深化彼此交流，並討論與日本應用場景串聯機會（目前日本有與柬埔寨討論如學位證書等各項資料的互通），以利數位皮夾國際應用場景擴充。

(二) Jay Kishigami（岸上順一）教授計畫在亞洲舉辦 Verifiable Credential workshop，主題是 VC use cases，時程約為今（113）年底或（114）明年初，據聞新加坡和泰國都有興趣參加，因其主題與我數位皮夾高度相關，將積極聯繫並評估實質參與。

(三) Wonsuk Lee 提及南韓的行動駕照採用 W3C VC 規格，目前負責的廠商應是 LG electronics（出席代表為 Hyojin Song），會後交流確認了相關技術規格並未公開於網路上，未來將持續聯繫是否能與南韓政府

開啟互通之討論。

- (四) 新加坡政府 Government Technology Agency (GOVTECH) 及 Infocomm Media Development Authority (資訊通信媒體發展局) 均參加本次 W3C 會議。GOVTECH 是發行 Singpass 的機關，已經完成將數項證件或文書之數位化 (例如學位證書)，但據其表示目前碰到的問題是缺乏驗證需求端 (沒有人要驗證使用)；Infocomm Media Development Authority 則採用 W3C VC 規格實作 TradeTrust 機制以為進出口使用，且 VC 的傳遞是透過電子郵件。與會時均向前述兩機關說明本部數位皮夾並尋求未來合作及互通之可能。

三、考量 W3C 的活動是全球性、開放性的，並可吸引來自世界各地的政府機關、企業和學術界的參與。政府部門參與其中，能夠建立起與其他國家和地區的合作關係，參與全球數位政策的制訂，提升國際影響力，並能夠確保自己所推動的數位服務和系統符合國際標準，避免因為標準落後而影響數位治理的推進。後續可評估規劃舉辦或參加 W3C 相關會議之建議如下：

- (一) 依據本次 TPAC 會議說明，W3C 將轉移部分組織發展費用於補助當地社群、活動、或課程等，此轉移將大幅影響既有 W3C Evangelist 之合作模式，亦為我國發展 W3C 周邊會議的新契機。
- (二) 本部數位皮夾現已規劃安排多場國際活動與會議，皆可考慮與 W3C 相關成員或專家接洽來訪，以利我國公共建設與國際標準發展組織之交流來往。

(三) 據本次會議與多位日籍專家學者了解，日本國內的 W3C 運作是以日本在 W3C 的員工為主，且部分費用是由 W3C 贊助，而 W3C 會員關係主管 Naomi Yoshizawa，本次也分享了在日本之 W3C 相關組織 WCAP，欲在亞洲地區舉辦 Web 技術相關課程，並說明此課程未來可以考慮與在地相關活動結合，譬如本部數位皮夾相關推廣活動、或其他民間之 Modern Web Conference 或 WebConf 技術研討會等，以利 W3C 相關組織與 Web 技術議題在臺灣生根。