異人研
Odditysay

2025 FEB.24 Monday —— VOL.001

# 隱私與信任的兩難

## 邁向數位身分自主的挑戰

*Decentralizing Trust*
*the Challenges of Implementing Self-Sovereign Identity*

# ✷ Event Highlights ✷

活動快訊

Mutual Support: Amplifying the Voices of Digital Rights Defenders in Taiwan and East Asia

RightsCon Satellite Events〖 衛星活動 〗

## 互助 - 共鳴 - 響亮：台灣與東亞數位人權之聲！

**地 點 Venue**
台北國際會議中心
Room 101C , (TICC)

**時 間 Time / Date**
9:00 - 12:30 , Feb. 24 , 2025

**Host 主辦單位**
開放文化基金會
Open Culture Foundation

✷

講座

## 隱私與信任的兩難：邁向數位身分自主的挑戰

Decentralizing Trust : the Challenges of Implementing Self-Sovereign Identity

**邀請國內外專家分享經驗，分析在推動身分自主，守護數位隱私的過程中，政策與科技分別扮演何種角色，以及面對哪些挑戰。**

Invite experts from Taiwan and abroad to share their insights and experiences, analyzing the roles that policy and technology play in advancing self-sovereign identity and safeguarding digital privacy, as well as the challenges encountered along the way.

**Speakers 與談人**

- 劉維人Warren Liu ·（異人研 Odditysay Labs）
- 周冠汝Kuan-Ju Chou ·（台灣人權促進會 Taiwan Association for Human Rights）
- Alexis Hancock ·（電子前哨基金會 Electronic Frontier Foundation）

---

在目前的數位化時代，我們的身分識別與資料授權幾乎完全依賴於集中式系統。無論是實體的政府證件還是線上的第三方平台。這些便利的架構逐漸累積隱憂：資料與足跡的不斷集中，使隱私洩漏風險激增並削弱使用者對資料與身分的掌控。

如今，以數位皮夾 （ Digital Identity Wallets ）與可驗證憑證 ( Verifiable Credentials, VC ) 為基礎的 Self-Sovereign Identity（身分自主）框架，為這個困境帶來新可能。它試圖用分散式的憑證取代集中的權威認證，推動資料最小化、使用者自主授權，讓資料真正回歸個人。

但這場轉型充滿未知與挑戰：分散式驗證框架，究竟能在那些環節，比既有的集中式驗證體系更方便、更安全？台灣又該如何汲取歐美等世界各國的經驗，探索適合本土的數位自主模式？

In today's digital era, identity verification and data authorization predominantly rely on centralized systems, such as government-issued IDs and third-party online platforms. While these systems offer convenience, they also exacerbate privacy risks by centralizing user data, thereby diminishing individual control.

The Self-Sovereign Identity (SSI) framework, leveraging Digital Identity Wallets and Verifiable Credentials (VCs), provides a decentralized alternative. By replacing centralized authorities with distributed credentials, SSI emphasizes data minimization and informed consent, empowering individuals to regain control over their personal data.Can decentralized verification match or surpass centralized systems in terms of convenience and security?

How can Taiwan draw on global best practices to design an SSI model that addresses local needs?

# ✷ 守護數位人權，需要個資控管工具 ✷

撰文者
Author

Warren Liu
劉維人

**為何數位身分很重要？因為隱私的保障與個資的控制權，是人權的基礎。**

- **何謂數位身分？ 以數位方式識別並應用的屬性 ＋ 存取資產與服務的權杖**
- **何謂隱私？ 我沒打算讓別人知道的屬性 ＋ 洩漏出去會造成嚴重衝擊的屬性**
  （無論是否僅涉及個人）

**要**保障數位人權與隱私，就不能把個人的屬性和足跡變成服務商的資產或戶政單位與稅務機關的專利。必須讓每個人都能控管自己的個資，同時，服務提供者必須能夠信任「每次前來存取服務&資料的人確實都是本人」。藉此防止偽冒詐騙，也防止服務提供者為了方便起見，蒐集更多足跡。

Kim Camaron 稱這個需求為 Identity Layer，主張數位世界充滿監控與偽冒，就是因為少了這層。要建立 Identity Layer，需要一個能夠自主控管身分與個資的工具。這個工具必須具備以下三種功能：

1. **泛用登入**：能夠用相同的識別符，連結各種個資、各種服務。
2. **自主授權**：能夠讓使用者決定要把哪些資料授權給誰，並留下某種紀錄確保服務提供者對於「**誰在哪裡同意了哪些東西**」具有共識。

   **知情同意**：能夠讓使用者以mental capacity能承受的方式，了解對方打算索取那些個資，拿去作什麼用，對自己可能有哪些影響。
3. **資料可攜**：能夠讓使用者把身分文件、服務紀錄、足跡等等拿出來，分享給自己授權的單位，並且可以阻止單位繼續使用。

GDPR這類隱私保護法規，與身分自主控制工具缺一不可。前者規範資料保管者行為，後者給予個人直接行使隱私權的能力。

所以歐盟除了制定GDPR，也制定了eIDAS，後者衍伸出了EUDIW，要求每一個會員國在2026年都打造出來免費給國民使用。自主控管身分與個資的工具，加上若干功能（信任框架、資料最小化、私鑰碎片化等等），可以達成以下效果：

- **每次使用個資皆需授權 + 使用者能夠隨時取消授權 = 防止個資濫用**
- **資料自主授權 + 自主攜帶 + 資料最小化 = 安全地獲得客製化服務**
- **相同的識別符 ＋ 由使用者決定揭露哪些個資/資料最小化 = 確認身分 + 防止追蹤**

值得一提的是，控制工具未必需要記載各種身分屬性。任何記載大量個資的工具（也就是由一個工具去滿足所有識別需求、客製化需求）都是危險的，因為這個功能意味著集中式資料傳輸節點（甚至集中式資料庫），會向全球駭客招手。同時，搞出一張可以控制所有重要證件的「至尊身分證件」（或「至尊身分控管工具」），可能也會增加無謂風險。這顆「魔戒」丟了會很麻煩，而且犯罪組織和極權國家一定會瞄準這顆「魔戒」來操弄。（他們也許無法入侵這顆「魔戒」，但可以用社交工程等方法欺騙使用者誤用）

比較好的方式，是把識別身分的證據能力分散在好幾個不同證件或機關，讓使用者只要蒐集夠多證據就能恢復身分。

物理世界中災難後的身份韌性就是這麼做的，目前的私鑰碎片化、皮夾復原等技術，也是用加密方法這麼做。

要實現身分韌性，就需要讓「證明身分」&「驗證身分」的資格盡量開放，且彼此互通。在理想上，應該讓所有公私立機構對身分識別、個資保管原則有相同的理解，讓每一方都知道各家證件的身分識別有多可信、保管的個資有多危險，藉此決定自己要使用哪些證件，索取哪些個資。這樣一來，就能防止任一證件獲得過大的權威性。

這樣的要求並不會妨礙商機。因為身分盜用與個資洩漏，使個資保管的成本不斷飆升。成熟企業並不喜歡保管大量個資，而是希望「需要使用個資的時候，可以輕鬆方便地拿到」。大企業的主要優勢也不在存放的大量個資，而是在平台上的強大服務。使用者可以自由攜帶個資，反而有利於他們催生更多客製化服務。新創與中小企業就更不用說了。使用者自由攜帶個資，可以讓他們拿到原本大企業牆內的資料，利用組織彈性推出更精準的服務。

總之，一個保障人權與隱私的數位世界，除了需要規範個資保管者與傳輸者的法規以外，也需要一個能讓所有人都自主控管個資授權的科技工具。這個工具需要以穩定但分散的識別符，連結各種可能的個資文件與服務商，授權所有個資的使用與處理，並且能夠自己決定將個資與足跡的檔案，從任何一個地方帶到其他別的地方。

關鍵詞
資料最小化 Data Minimization
資料可攜 Data Portability
信任框架 Trust Framework
身分的可組合性 Composability of Identity
使用者自主授權 informed consent

# Empowering Digital Rights:

## Self-Sovereign Identity and the Future of Data Control.

*The Role of Personal Data Management Tools in Protecting Digital Human Rights.*

Author
Warren Liu

### The Importance of Digital Identity

In an era of deepening digitalization, privacy protection and personal data control have become fundamental human rights. Digital identity plays a crucial role in safeguarding these rights, ensuring that individuals retain autonomy over their information while accessing various digital services.

A digital identity comprises multiple attributes used to identify individuals online, combined with digital credentials that authorize access to assets and services. It enables seamless interaction with digital platforms while maintaining security and credibility. Privacy, on the other hand, pertains to attributes that individuals choose not to disclose. If exposed, such information can lead to significant personal or institutional damage. Protecting privacy requires robust systems that empower individuals to control their data while preventing unauthorized access.

To uphold digital rights and privacy, personal attributes and digital footprints should not become the property of service providers or be monopolized by government agencies such as civil registries or tax authorities. Every individual should have the autonomy to manage their own data and decide which information to share and with whom. At the same time, service providers must ensure that each access request is authenticated to prevent fraud and should collect only necessary data rather than amassing information for convenience. Kim Camaron introduced the concept of the "Identity Layer," asserting that the prevalence of surveillance and fraud in the digital world stems from the absence of such a layer. Establishing an identity layer is, therefore, critical to protecting individual digital rights.

### Key Elements in Building an Identity Layer

Creating an identity layer requires tools that support self-sovereign identity (SSI) and data management, incorporating the following key features.

1. ***Universal Login***: A consistent identifier that links personal data across various services.

2. ***User-centered Authorization***: Allows users to decide which data to share and with whom, while keeping records to ensure agreement on "who consented to what and where."

   **Informed Consent**: Ensures that users understand the data being requested, its intended use, and its potential impact in a manner appropriate to their mental capacity.

3. ***Data Portability***: Enables users to securely share identity documents, service records, and digital footprints with authorized entities while maintaining the ability to revoke access.

Privacy regulations such as the European Union's General Data Protection Regulation (GDPR) complement SSI tools. GDPR establishes guidelines for data custodians, while SSI empowers individuals to exercise their rights. This synergy has driven the development of the EU's eIDAS initiative and the European Digital Identity Wallet (EUDIW), which mandates that all member states provide free digital identity tools by 2026.

---

### The Importance of Digital Identity

When SSI tools are combined with features such as trust frameworks, data minimization, and privacy-enhanced cryptographic technology, they offer multiple benefits.

- Preventing data misuse - every use of personal data requires explicit authorization and on-demand revokability.
- Ensuring both security and personalized services - With user-centered data authorization, portability, and minimization, individuals can access tailored services without unnecessary data exposure.
- Enabling identity verification without tracking - by using a consistent identifier while allowing users to control what information they disclose and minimize data exposure, allows for authentication while preventing unwanted tracking.

## Principle of Identity Resilience

It is important to note that identity management tools do not necessarily need to store all identity attributes. To ensure the robustness of digital identity systems, several fundamental principles should be followed.

- Centralized data storage should be avoided, as housing all identity attributes in a single system creates a prime target for cyberattacks.
- Additionally, the concept of an "all-powerful identity card" should be rejected, as consolidating all credentials into a single tool (“the One Ring to rule them all") introduces risks of social engineering attacks and government overreach. Instead, identity verification should be distributed across multiple documents or institutions to enhance resilience. For instance, multi-party computation and digital wallet recovery technologies use cryptographic methods to ensure security.

## Building Identity Resilience

A resilient identity ecosystem requires open and interoperable verification mechanisms to ensure compatibility while maintaining high security standards. Collaborative standards further strengthen the ecosystem by encouraging public and private sectors to adopt shared principles for identity verification and data protection, preventing any single credential from becoming overly authoritative.

## Balancing Security and Innovation

These requirements do not hinder business opportunities. By reducing the risks associated with centralized storage, it effectively lowers financial costs related to data breaches and identity theft. Established companies prefer not to store excessive personal data but instead seek efficient ways to access necessary information when needed. Their competitive advantage lies not in hoarding data but in providing powerful and practical services to their customers. Meanwhile, data portability fosters innovation, allowing businesses to offer enhanced services without monopolizing user data. Additionally, breaking down data silos enables startups and small to medium-sized enterprises (SMEs) to access information previously controlled by large corporations, fostering niche market services.

## Conclusion: The Path Forward

To build a digital world that respects human rights and privacy, legal and technological advancements must progress hand in hand. Laws should regulate data custodians and transmitters to prevent misuse, while technological tools should empower individuals to manage their data access autonomously. Effective digital identity tools should utilize stable yet decentralized identifiers to connect personal data and services. Moreover, consent-based data usage and processing mechanisms should be established to enhance transparency and security, enabling users to securely transfer and control their digital identity data while maintaining full ownership of their information.

The discussion is just beginning. Feel free to share your feedback with us at **warren@oddítysay.org**.

*Shoutout to Yun Yan for proof-reading!*

Key Words: Data Minimization, Trust Framework, Data Portability, Composability of Identity, Informed Consent

Oddítysay

探索科技、隱私與信任之間的權衡。

*Exploring the trade-offs between technology, privacy, and trust.*

**創新 Innovation / 監管 Regulation**

開放系統促進創新，但如何與既有憑證體系共存？ / SSI serves as both a digital identity system and a trust framework—but can technology alone establish trust?

**便利 Convenience / 隱私保護 Privacy Protection**

SSO 登入順暢，但也追蹤使用足跡，怎麼辦? SSO simplifies access, but at what cost to privacy ?

**客製化 Personalization / 個資保護 Data Protection**

我們值得為了更貼身的使用體驗，交出自己的個資嗎? / Customized services enhance user experience, but should personal data be commodified?

# 這些真的無法兼顧嗎 還是只是看似矛盾的假議題

Are these truly dilemmas, or are some of them false trade-offs

**科技 Technology / 社會信任 Social Trust**

SSI 既是數位身份，也是信任架構，但科技能單獨建立信任嗎？ / SSI serves as both a digital identity system and a trust framework—but can technology alone establish trust?

**使用者控制 User Control / 隱藏風險 Hidden Risks**

勾選 EULA 真的代表知情同意嗎？ / Does agreeing to an EULA mean true informed consent?

**安全 Security / 反監控 Anti-Surveillance**

更強的安全措施通常伴隨更高的監控，我們該如何拿捏界線？ / Stronger security measures often come with increased surveillance—where do we draw the line?

---

在數位時代，如何安全管理個人的身分與資料？異人研是一個由社會科學研究者與技術專家組成的團隊，以創新技術實現社會需求為使命，重視以資料最小化與使用者自主授權等核心原則，希望推動更安全、流暢且可信的數位生態系。目前，我們參與台灣數位發展部的數位皮夾研析計畫，深入研究如何透過分散式識別符 (decentralized identifiers, DIDs)、可驗證憑證/可驗證展示(verifiable credentials/presentations, VCs/VPs) 等先進技術，以及相應的制度設計，實現身分自主 ( Self-Sovereign Identity, SSI ) 。

Odditysay


劉維人 warren@odditysay.org
曾郁珊 zoey@odditysay.org
廖珮杏 peixing@odditysay.org


As the digital age progresses, securely managing identities and personal data has become an urgent challenge. Odditysay Labs is a research team comprising social science researchers and technology experts dedicated to developing innovative solutions to address societal needs. Guided by principles such as data minimization and informed consent, we envision a safer, more seamless, and trustworthy digital ecosystem. Currently, we are collaborating with Taiwan's Ministry of Digital Affairs on the Digital Identity Wallet Research and Analysis Project. This initiative explores how advanced technologies — including Decentralized Identifiers (DIDs), Verifiable Credentials (VCs) / Verifiable Presentations (VPs), and well-designed institutional frameworks—can collectively realize the vision of Self-Sovereign Identity (SSI). By examining the intersection of cutting-edge technology and governance models, we seek to explore a resilient, locally adapted SSI framework for Taiwan.