自我主權身份 (Self-Sovereign Identity, or SSI) 原則

這些 SSI 的基本原則適用於任何數碼身份生態系統使用。歡迎任何機構將這些原則納入其數碼身份生態系統治理框架 中，並在納入時保證其完整性。SSI的及基本原則僅受相關司法管轄區的官方法律及法規限制。

1. 代表性 (Representation)

SSI 生態系統應為任何實體 (包括人類、法定、自然、實質或數碼) 提供相應方法，使其可以獲取何數量對其有代表性的數碼身份。

2. 互相操作性 (Interoperability)

SSI 生態系統應使用開放、公共和免版稅的標準互相操作，使實體的數碼身份訊息可在跨系統操作時仍具代表性，並在系統間實現互換、安全防衛、訊息保護和驗證。

3. 去中心化 (Decentralization)

SSI 生態系統不應要求依賴集中式系統 (centralized system) 來代表、控制或驗證實體的數碼身份訊息。.

4. 控制與代理機構 (Control and Agency)

SSI 生態系統應賦予具有自然、人類或法定權利的實體，成為“身份權利持有方” (Identity Rights Holder)， 可以控制其數碼身份訊息的使用，並通過僱用和/或委託其選擇的代理端 (Agent) 和監護人 (Guardian) -- 包括個人、機構、設備和軟件 -- 行使這種控制權。

5. 參與性 (Participation)

SSI 生態系統不應強制身份權利持有方參與。

6. 平等與包容 (Equity and Inclusion)

SSI 生態系統不得在其治理範圍內排斥或歧視身份權持有方。

7. 可用性、無障礙環境和一致性 (Usability, Accessibility and Consistency)

SSI 生態系統應為身份權利持有方最大化代理端和其他SSI組件的可用性和無障礙環境，包括一致性的用戶體驗。

8. 可轉移性 (Portability)

SSI 生態系統不應限制身份權利持有方將其數碼身份訊息的副本移動或轉移到他們選擇的代理端或系統上。

9. 安全性 (Security)

SSI 生態系統應賦予身份權利持有方保護其靜態和動態的數碼身份訊息的能力，並控制其本身的識別標籤 (identifier) 和加密匙 (encryption key)，以及對所有互動採取端對端加密 (end-to-end encryption)。

10.可驗證性和真實性 (Verifiability and Authenticity)

SSI 生態系統應賦予身份權利持有方能提供可驗證證據 (verifiable proof)，以證明其數碼身份訊息的真實性。

11.隱私保護和最少訊息披露 (Privacy and Minimal Disclosure)

SSI 生態系統應允許身份權利持有方保護其數碼身份訊息的隱私，並分享任何特定互動所需的最少數碼身份訊息。

12.透明度 (Transparency)

SSI 生態系統應允許身份權利持有方和所有其他利益相關者輕鬆取得和驗證必要的信息，以了解SSI生態系統的代理端和其他SSI 系統組件運作的動機、規則、政策和演算法。

本文件由全球SSI社區成員開發，由Sovrin基金會召集並作為這些原則的管理者。

本文件由Sovrin基金會維護，並經由Sovrin董事會批准，可納入Sovrin實用程序治理框架和Sovrin生態系統治理框架。

我們邀請您對本文件的社區版提供任何評論或建議 -- 本文件開放給任何人。

如果您有興趣參與SSI原則的持續開發，請訪問Sovrin治理框架工作組會議專頁。

SSI原則獲得以下機構的認可及支持：