自主身份（Self-Sovereign Identity, or SSI）原则

本文档中自主身份 (SSI) 的基本原则适用于任何数字身份生态体系。我们鼓励任何构建数字身份生态系统的机构把这些原则纳入其治理框架，并且在纳入时保证其完整性。这些基本原则的应用只应在与相关法律及法规有出入时受到限制。

1. 代表性 (Representation)

自主身份（SSI）生态系统应该为任何实体（包括人类、法律实体、自然实体、物质实体和数字实体）提供相应方法，使其可以获得任意数量对其有代表性的数字身份。

2. 互相操作性 (Interoperability)

自主身份（SSI）生态系统应该使用开放的、公用的以及无版税的标准，使实体的数字身份信息可以在跨系统操作时仍旧具有代表性，并且可以在系统间实现互换、安全防卫、信息保护以及跨系统验证。

3. 去中心化 (Decentralization)

自主身份（SSI）生态系统不应有任何要求使其参与者必须要依赖集中式系统（centralized system）来代表、控制及验证一个实体的数字身份信息。

4. 控制及代理 (Control and Agency)

自主身份（SSI）生态系统应赋能具有自然、人类及法律权利的实体，使其 作为“身份权利持有方 （Identity Rights Holder）”可以对与其身份相关的数字身份信息的使用进行控制，并通过使用或者放权给其自己选择的代理方（Agent）和监护方（Guardian）来实施控制。代理方和监护方可以是个人、机构、设备和软件。

5. 参与性 (Participation)

自主身份（SSI）生态系统不应强制身份权利持有方参与。

6. 平等与包容 (Equity and Inclusion)

自主身份（SSI）生态系统不得排斥或歧视其治理范围内的任何身份权利持有方。

7. 可用性、无障碍性及一致性 (Usability, Accessibility and Consistency)

自主身份（SSI）生态系统应该为身份权利持有方最大化代理方以及系统其他组成部分的可用性和无障碍性，包括用户体验的一致性。

8. 可转移性 (Portability)

自主身份（SSI）生态系统不应限制身份权利持有方对其数字身份信息副本进行移动或转移至其所选代理方或系统的能力。

9. 安全性 (Security)

自主身份（SSI）生态系统应赋能身份权利持有方，使其数字身份信息的安全在静态和动态时都得到保证，并且给予身份权利持有方对其身份识别码（identifier）和密钥（encryption key）的控制，让其在所有交互中都可以采用端到端加密（end-to-end encryption）。

10. 可验证性和真实性 (Verifiability and Authenticity)

自主身份（SSI）生态系统应赋能身份权利持有方，使其可以提供可验证凭证 (verifiable proof)，来证明其数字身份信息的真实性。

11. 隐私保护及最小化信息披露 (Privacy and Minimal Disclosure)

自主身份（SSI）生态系统应赋能身份权利持有方，使其可以保护其数字身份信息的隐私性，并且允许其在任何特定交互中只提供该交互所必须的最少数字身份信息。

12. 透明度 (Transparency)

自主身份（SSI）生态系统应赋能身份权利持有方以及其所有利益相关方，使他们可轻松获得并验证所需信息，以理解所有代理方以及其他自主身份生态系统组成部分赖以运作的激励措施、规则、政策和算法。

本文件由Sovrin基金会维护，并经Sovrin理事会批准，可納入Sovrin实用设施治理框架和Sovrin生态系统治理框架。

我们邀请您对本文件的社区维护版提供评论或建议 -- 本文件对所有人开放。

如果您有兴趣参与“自主身份（SSI）原则”的持续开发，请访问Sovrin治理框架工作組会议专页。

自我身份（SSI）原则获得以下机构的认可及支持：