EXECUTIVE SUMMARY

The T3 Innovation Network™ (T3 Network) comprises more than 500 organizations working together to build an open, decentralized, public-private infrastructure for a more equitable talent marketplace where (1) all learning counts, (2) competencies and skills are currency, and (3) learners are empowered with their own data. A project within the T3 Network—Management and Use of Individual-Level Data Records—developed a charter to explore open, self-sovereign protocols and data management guidance for interoperable learning records (ILRs), which is the focus of the paper on “Applying Self-Sovereign Identity Principles to Interoperable Learning Records.”

The term “self-sovereign” arises from the term “self-sovereign identity” (SSI), which is associated with both a set of technical standards and a set of community-promulgated principles seeking to enable a shift toward more individual control over digital identities and personal data. The design of SSI-type systems provides a lens to examine how we might restructure such systems to be more equitable, giving learners better access to, and control over, the management of their learning records while maintaining the verifiability of this data. SSI-based approaches could more readily recognize and empower learners while simultaneously improving educators’ abilities to teach and employers’ and recruiters’ abilities to find workforce candidates who suit their needs.

Interest in portable, interoperable, verifiable digital records has expanded in response to COVID-19. At the same time, proposed solutions such as immunity credentials have brought increased awareness of the need to ensure individual rights and privacy in the process. SSI is not a fully formed solution to these concerns. However, individual rights and privacy has been a primary focus of SSI, building on decades of expertise of individuals in the identity space. As such, SSI technologies and concepts can provide valuable insights to jumpstart our efforts and provide opportunities to improve the talent marketplace for all learners and stakeholders by examining ILR systems’ potential risks, such as discrimination, manipulation, over-disclosure, tracking, and lock-in/lock-out. Stakeholders should be encouraged to work toward and implement the following principles and tools, when possible, to mitigate risks that are further explained throughout the paper and highlighted below.

- **Verifiable Credentials**—support flexible proof mechanisms to ensure the credentials are cryptographically reliable and that the issuing institution stands by the statements contained therein and suspends or revokes issued credentials if necessary.
- **Decentralized Identifiers**—provide a means for both institutions and learners to establish identity without reliance on a centralized party.
• Decentralized Verifiable Data Registries—publish the status of suspended or revoked credentials without requiring verifiers to contact the original issuing authority.

• Privacy-Promoting Credential Status Checks—inspect the current status of a credential without revealing any additional personally correlatable data about the individual.

• Personal Data Stores—provide standards and protocols to support individual control over sharing and access to their data.

• Selective Disclosure—allow an individual the option to share parts of a larger data set.

• Elective Computation—ensure that any processing of an individual’s information is explicitly requested.

• Progressive Disclosure—share the minimal amount of information initially and gradually share more information as the value proposition becomes clearer, rapport is built, and trust is developed.

• Embedded Identity Proofing Attributes—include personally identifiable information directly in a credential, only when necessary and appropriate, to ensure usefulness of these standards with digital identity frameworks.

• Minimizing Collected Data—request the absolute minimum information for any particular transaction.

• Information Fiduciaries—support parties with a legally binding obligation to act in the interest of individuals with regard to the acquisition, processing, and distribution of personal information.

• Governance Frameworks—create structures, roles, and policies of an organization or government to adapt SSI approaches to different domains, resolving questions of trust within different stakeholder groups.

The paper further provides technical details of SSI standards and technologies to describe how implementers (such as ILR pilots supported by the T3 Network) can begin applying technical solutions (as described above) to promote self-sovereign management of individual-level data records. Additionally, talent marketplace ecosystems, like the T3 Network, play an important role in developing governance frameworks and promoting sustainable growth of networks committed to self-sovereign management of learner records and learner privacy, while ensuring ethical, equitable outcomes for learners. ILR pilots and other stakeholders should consider utilizing and further testing the principles, technologies, and community guidance outlined in this paper in low-risk, isolated environments and share their findings and best practices with the T3 Network and broader SSI community.