FISE Technologies White Paper

Authored By

M.E. ‘Nara’ Lau, CEO, FISE Technologies Inc.
nara@fisetech.ai

Kevin W. Hartig, CTO, FISE Technologies Inc.
kevin@fisetech.ai

Publication Date(s):

5 June 2023 v1, 14 June 2026 v1.1

Copyright Notice and Intellectual Property Statement

The framework architecture, platform design, technical specifications, proprietary methodologies, and original concepts described in this white paper are the exclusive intellectual property of FISE Technologies and are protected under applicable U.S. and international intellectual property, patent, copyright, and trade secret laws. This document is provided for informational purposes only and does not constitute a legal agreement, offer, or warranty of any kind. Unauthorized reproduction, distribution, modification, or commercial use of any content contained herein is strictly prohibited without the prior written consent of FISE Technologies. Third-party standards, protocols, and specifications referenced herein remain the intellectual property of their respective owners and are cited solely for contextual and technical reference purposes.

Email inquiries regarding FISE Technologies' permissions, licensing, or proprietary use: info@fisetech.ai

Table of Contents

Abstract

This white paper describes FISE Technologies' platform, Signet (https://signetapp.cloud), and establishes the need for a new foundational framework, one that supports the standardized development of Self-Sovereign Identity (SSI) applications across digitized environments such as the internet and health data devices.

A range of both legacy and emerging technologies exists to securely host and self-manage personal data, defining how and when it can be shared directly between peers. Mechanisms are available to acquire, manage, and validate credentials that define specific attributes of individuals and entities. Additional tools support the creation and management of decentralized IDs, decentralized storage, and cryptocurrency.

Currently, few implementations integrate these foundational components into a unified interface, one that enables individuals to securely interact across multiple applications and with diverse individuals, organizations, and trusted entities. Today's non-interoperable applications remain largely siloed, built on custom implementations that cannot seamlessly communicate with one another. The solution is a common framework that replaces antiquated silos with user-centric, interoperable integration of applications and services, empowering users and organizations to seamlessly manage their digital identities and data.

The framework proposed in this white paper encompasses key infrastructure components and services including streamlined sign-up and onboarding, unique decentralized ID assignment, a cryptocurrency wallet, verifiable credentials management, and decentralized storage access. These components form the cornerstones of the framework. FISE Technologies integrates and interoperates these infrastructure elements, enabling users to store and manage IDs, data, credentials, and currency in one cohesive ecosystem.

FISE Technologies' framework connects these components through software libraries and APIs, empowering developers to build custom applications that allow users to securely access their assets via trusted, individually defined interactions. FISE Technologies' platform, Signet, operationalizes self-sovereign identity principles, introducing a transformative approach to identity management, user-controlled privacy, built-in security, and personal data sovereignty. This white paper elaborates on FISE Technologies' proposed SSI framework, its implementation, essential use cases, current challenges and limitations, and detailed descriptions of its technical components.

I. Introduction

Current Challenges in Managing Digital Identities

To develop tools that facilitate self-sovereign identity, users must be empowered to own and manage one or more identifiers. On a sliding scale of granularity, the most granular definition of a user is the individual, with broader entity user representations spanning sole proprietors, small businesses, corporations, consortiums, and governments.

When digital self-sovereignty is respected, enforced, and maintained at the individual user level, it naturally extends to entity users — spanning sole proprietors, small businesses, corporations, consortiums, and governments. Conversely, when individual users' digital self-sovereignty is ignored, abused, or violated, entity users suffer the same consequences. The individual is the most fundamental building block of any entity and, by extension, the most critical foundation of any sustainable and thriving economy.

Today, individuals universally possess some form of identification that establishes their identity. Digital identifiers have already achieved widespread adoption for representing both individuals and entities. Online accounts using username and password credentials represent a prevalent form of digital identification, yet ownership and control remain with third-party service providers rather than the individuals they identify.

Centralizing identity data across siloed data centers and storage systems is inherently problematic. Current implementations of digital identity management systems (IMS) have experienced, and continue to risk, the following issues:

- **Identity Theft and Fraud:** Identity theft is a crime in which someone weaponizes another person's personal information to commit fraud or other crimes. It can have a devastating and long-lasting impact on victims and is extremely difficult to recover from. Cybercriminals continuously exploit new technologies and tactics to steal personal information, making it increasingly difficult to verify the authenticated identity of users. In 2024, it was reported that identity theft, fraud, scams, AI-enabled attacks, and massive data breaches affected over 75 million Americans, costing $47 billion, a 9% increase from 2023's combined losses of $43 billion.[1]
- **Data Breaches:** Large-scale data breaches are a major and growing threat to digital identities. They expose sensitive information such as passwords, Social Security numbers, and medical records, which cybercriminals exploit to commit identity theft and fraud. Data breaches occur with alarming frequency across virtually every type of organization. In 2025, U.S. data breaches hit a record 3,322 incidents, with 1.7 billion individuals having their personal data compromised, a 312% increase from 2023.

[1]Javelin Strategy & Research & AARP. (2025, March). Identity fraud and scams cost Americans $47 billion in 2024. AARP. https://www.aarp.org/money/scams-fraud/javelin-identity-theft-report-2024/; Gen Digital & LifeLock. (2026, January). 53 key identity theft statistics for 2026. LifeLock. https://lifelock.norton.com/learn/identity-theft-resources/how-common-is-identity-theft

Industries affected include oil & gas, motor vehicles, IT, telecom, social media, retail, healthcare, financial services, government, and critical infrastructure.[2]

- **User Experience:** Users demand a convenient and seamless experience when using digital services, yet this remains difficult to achieve without compromising data security. A 2025 analysis of over 19 billion exposed passwords found that 94% are reused or duplicated across multiple accounts, leaving users critically vulnerable to credential stuffing attacks. Despite advances in authentication technology, over 80% of users still reuse passwords in some form, with the most common passwords remaining dangerously weak. Password lists stored in unsecured locations continue to be easily exploited, and even dedicated password managers have proven vulnerable — most notably when LastPass settled a class action lawsuit in 2025 for $24.5 million following a breach that compromised the vault data of over one million users. Most critically, users remain largely unaware of where their personal information is stored, who controls it, or how to manage it effectively.[3]
- **Interoperability:** Digital identities are increasingly used across multiple platforms and systems. While federated identities may suffice for a limited set of collaborating services, they create significant challenges for broader interoperability and compatibility. Federated identities operate only within a restricted ecosystem of services, leaving users with little transparency into where their identity information is stored, how it is shared, or how it is ultimately used.[4]
- **Regulatory Compliance:** Organizations must navigate a rapidly expanding landscape of regulations and standards governing data privacy and security, making compliant digital identity management increasingly complex — particularly where regulations conflict with one another. Today, more than 170 countries have enacted data privacy regulations, with new laws introduced each year. By 2025, over 20 U.S. states had enacted comprehensive privacy laws, while GDPR fines reached €20 million and CCPA penalties expanded under the CPRA. Current regulatory compliance standards organizations must accommodate include GDPR, CCPA/CPRA, KYC, FCPA, PCI-DSS, ISO standards, and an ever-growing body of regional and sector-specific legislation.[5]

---

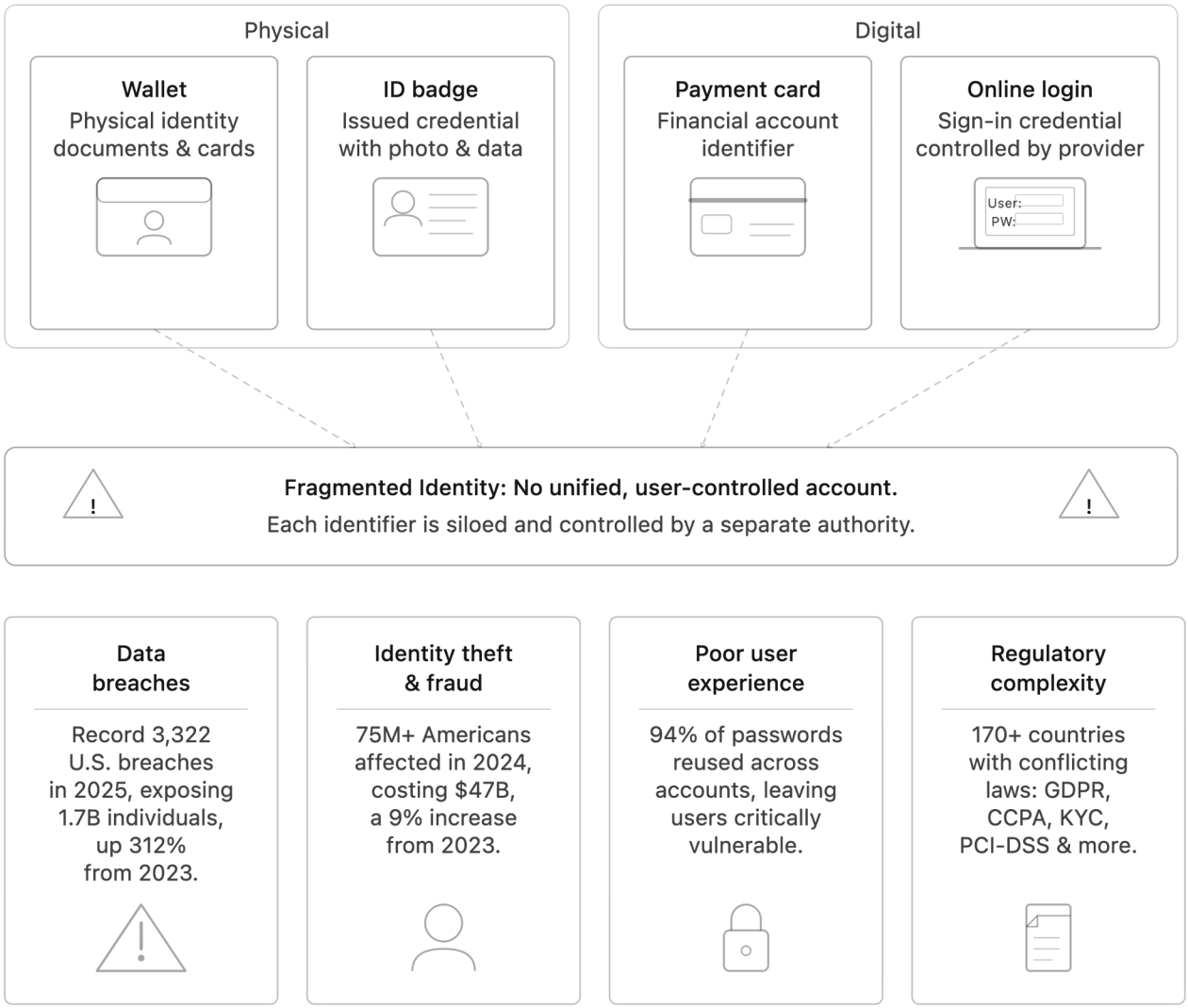
[2] StationX. (2026). Biggest data breaches in history. StationX. https://app.stationx.net/articles/biggest-data-breaches; DeepStrike. (2026). Data breach statistics 2025–2026: Global trends & costs. DeepStrike. https://deepstrike.io/blog/data-breach-statistics-2025

[3] Cybernews & CinchOps. (2025, May 1). Password leak study unveils alarming 2025 trends: 94% of passwords reused. CinchOps. https://cinchops.com/password-leak-study-unveils-alarming-2025-trends-94-of-passwords-reused/; DeepStrike. (2026, April). Password statistics 2026: Reuse, breaches, MFA & passkeys. DeepStrike. https://deepstrike.io/blog/password-statistics-2025; Wikipedia. (2025). LastPass 2022 data breach. Wikipedia. https://en.wikipedia.org/wiki/LastPass_2022_data_breach

[4] Aldosary, M., & Alqahtani, N. (2021). Federated identity management (FIdM) systems limitation and solutions. arXiv. https://arxiv.org/pdf/2104.14018; Identity Management Institute. (2021). Federated identity management challenges. https://identitymanagementinstitute.org/federated-identity-management-challenges/

[5] Usercentrics. (2025, March 25). Global data privacy laws: Your 2025 guide (GDPR, CCPA, more). Usercentrics. https://usercentrics.com/guides/data-privacy/data-privacy-laws/; Secure Privacy. (2025, July 30). First-party data collection & compliance: Best practices. Secure Privacy. https://secureprivacy.ai/blog/first-party-data-collection-compliance-gdpr-ccpa-2025

Diagram 1: Current Challenges in Managing Digital Identities

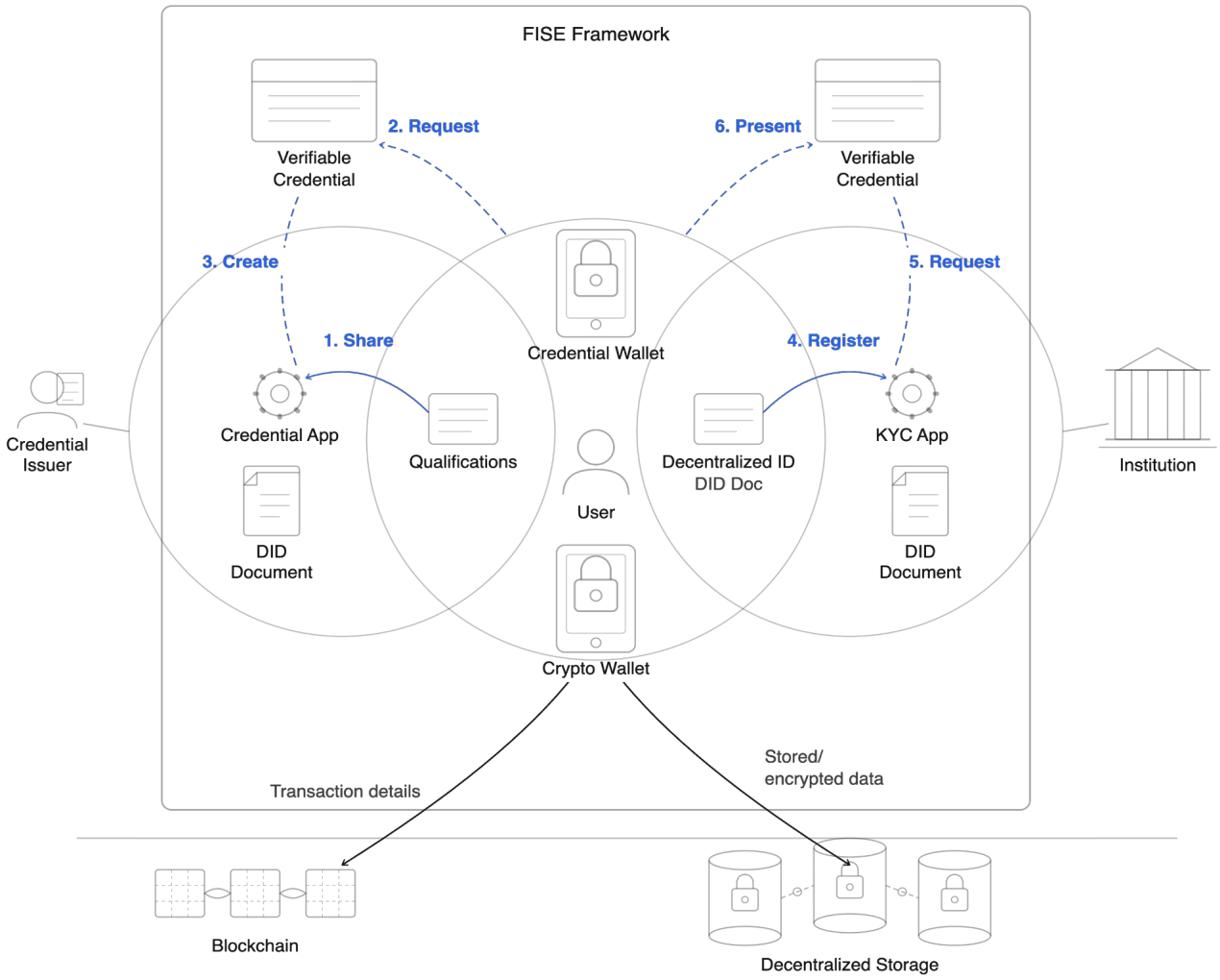


The Need for a New Approach to Identity Management

The limitations of traditional identity management systems are directly addressed by implementing a **self-sovereign identity** (**SSI**) platform. An SSI platform is a decentralized system that empowers individuals to own and control their identity, credentials, data, and currency in one unified place and from a single context. This information can be selectively

shared to verify identity with websites, services, and applications — eliminating reliance on a central authority as an intermediary for every interaction.[6]

Diagram 2: FISE Framework, New Approach to Identity Management



[6] Dock.io. (2026). *Self-sovereign identity: The ultimate guide 2026*. Dock. https://www.dock.io/post/self-sovereign-identity; Cardano Foundation. (2025, December 19). *A strategic guide to self-sovereign identity*. Cardano Foundation. https://cardanofoundation.org/blog/ssi-rebuilding-digital-trust

FISE's SSI platform addresses the limitations of traditional identity management systems in the following ways:

- **Privacy**: User data is stored in a decentralized manner, cryptographically signed to indicate ownership and encrypted to ensure it remains private, secure, and accessible only to authorized parties.
- **Security**: An SSI platform is architected with built-in, layered security measures that leverage advanced cryptographic techniques for authentication, authorization, and comprehensive data management.
- **User Control**: Users retain complete, granular control over their identity data — with the ability to create, access, update, and delete their data at any time, without third-party intervention.
- **Common Framework**: An SSI platform provides a standardized framework for building SSI-based applications, lowering the barrier for developers to create new solutions while simplifying how users manage the applications they rely on.
- **User-Friendly UI**: An SSI platform delivers an intuitive, unified interface for users to seamlessly manage their identities, credentials, storage, documents, data, NFTs, and cryptocurrencies in one place.

The FISE Framework provides a more secure, private, authenticated, and user-controlled approach to identity management, purpose-built for the demands of today's digital landscape.

II. FISE Technologies' Problem Statement

Traditional identity management systems suffer from a number of limitations, including:

- **Privacy:** Existing solutions commonly rely on centralized authorities, meaning user data is rarely fully private. In centralized and federated identity management systems, identity data is owned and controlled by identity providers, not the identity subjects themselves. This creates conditions for data breaches, identity theft, and systemic privacy violations. Personal user data is frequently mined and sold for profit with little or no consideration for the individual whose data is at stake.[7]
- **Security:** Centralized authorities represent a single point of failure. If a central authority is breached, the personal data of users under management is potentially compromised, making large-scale exposure an inherent structural risk rather than an isolated incident.[8]

[7] Mazzocca, C., Bernabeo, A., Bistarelli, S., & Di Battista, G. (2025, April 16). *A survey on decentralized identifiers and verifiable credentials.* arXiv. https://arxiv.org/abs/2402.02455
[8] Mazzocca, C., Bernabeo, A., Bistarelli, S., & Di Battista, G. (2025, April 16). *A survey on decentralized identifiers and verifiable credentials.* arXiv. https://arxiv.org/abs/2402.02455

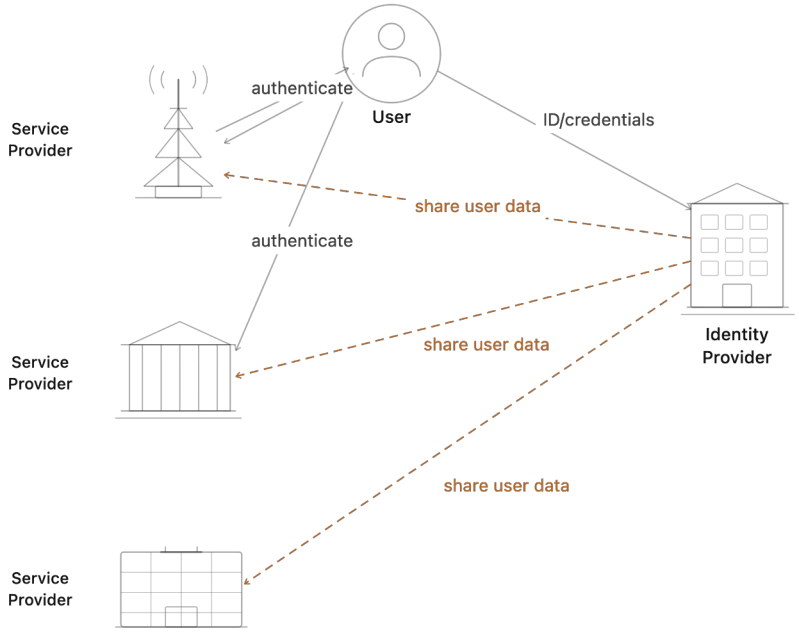
- **User Control:** Users have limited control over their identity data in traditional systems, making it difficult to access, update, or delete their information. Some jurisdictions have enacted laws requiring companies to honor individuals' data management requests, yet how to submit such requests is rarely obvious or intuitive. Fulfilling these requests is often time-consuming and procedurally unclear, and in many regions users have no legal recourse to manage their own personal data whatsoever.[9]
- **Lack of a Common Framework:** A significant gap persists in software design patterns for decentralized identity. No cohesive framework currently exists that seamlessly integrates verifiable credentials, decentralized IDs, decentralized storage, and cryptocurrency, the critical components of a unified, user-centric foundation for the development of decentralized applications (DApps). While decentralized identifiers (DIDs) and verifiable credentials (VCs) have been standardized by the World Wide Web Consortium (W3C), achieving trusted identity verification and data sharing without compromising privacy remains a significant challenge.[10]
- **Insufficient UIs:** The absence of a cohesive, intuitive user interface continues to hinder convenient, user-centric management of identities, credentials, storage, documents, data, NFTs, and cryptocurrencies. This lack of accessibility impedes the mass adoption of digitized ownership, decentralization, and data sovereignty at scale.[11]

[9] Xobee Networks. (2026, February). *Decentralized identity management frameworks: The ultimate guide for digital identity in 2025.* https://xobee.com/2025/04/decentralized-identity-management-frameworks-the-ultimate-guide-for-digital-identity-in-2025/

[10] W3C. (2022). Decentralized identifiers (DIDs) v1.0. https://www.w3.org/TR/did-core/; Yuan, H. et al. (2025, October). A scalable, privacy-preserving decentralized identity and verifiable data sharing framework based on zero-knowledge proofs. arXiv. https://arxiv.org/abs/2510.09715

[11] Xobee Networks. (2026, February). *Decentralized identity management frameworks: The ultimate guide for digital identity in 2025.* https://xobee.com/2025/04/decentralized-identity-management-frameworks-the-ultimate-guide-for-digital-identity-in-2025/

Diagram 3. Federated Identity Management. User data centrally controlled by custodian.



III.Solutions: FISE Framework

Self-sovereign identity (SSI) is a transformative approach to identity management that gives users direct, verifiable control over their own identity data. SSI leverages decentralized technologies including blockchain, distributed storage, verifiable credentials, and advanced identity creation protocols to manage a comprehensive portfolio of personal data. The SSI market is projected to grow from $1.30 billion in 2024 to $44.98 billion by 2032, registering a compound annual growth rate of 84.5%, driven by the exponential rise of digital transformation, blockchain technology, and zero-trust identity architectures.[12] This decentralized approach offers significant advantages over traditional centralized identity management systems, including:

- **Increased Security:** SSI substantially reduces the susceptibility of user identities to theft and unauthorized access. SSI eliminates centralized identity storage, reducing fraud risk and data breaches, and enhances compliance with data protection laws such as GDPR, CCPA, and Japan's APPI. Dynamic cryptographic techniques encrypt and protect user data, rendering it highly inaccessible to unauthorized parties.[13]

[12] DataM Intelligence. (2025, November 5). Self-sovereign identity (SSI) market to reach USD 44.98 billion by 2032, driven by blockchain adoption and privacy regulations. PR Newswire. https://www.prnewswire.com/news-releases/self-sovereign-identity-ssi-market-to-reach-usd-44-98-billion-by-2032--driven-by-blockchain-adoption-and-privacy-regulations--datam-intelligence-302605546.html

[13] DeepStrike. (2025, December 7; updated 2026, April 23). Data breach statistics 2025–2026: Global trends and insights. DeepStrike. https://deepstrike.io/blog/data-breach-statistics-2025

- **Improved Privacy:** SSI gives users granular control over their personal information, including what data they share, with whom, and for how long. In an SSI framework, individuals maintain ownership of their identity attributes, which are cryptographically secured and can be selectively shared with authorized entities, enhancing user privacy and reducing the risk of large-scale data breaches.
- **Enhanced Portability:** SSI enables seamless portability, allowing users to carry their identity data across different systems and platforms. Because SSI data is stored in a decentralized, standards-based format, it is not bound to any single system, provider, or jurisdiction.[14]
- **Better User Experience:** SSI allows users to manage identity information in digital wallets, selectively sharing portions of that data using cryptographically verifiable credentials, providing an intuitive, user-centric way to manage an identity portfolio without requiring technical expertise.

The need for next-generation identity management systems built on SSI technologies is urgent and unambiguous. Enterprises and governments are recognizing the inadequacies of traditional centralized systems for identity management, particularly given the rising frequency of data breaches and identity theft. Current systems lack sufficient security, frequently fail to meet evolving regulatory standards, and perpetuate unethical digital experiences that expose users daily to identity theft, fraud, and exploitation.[15]

FISE Technologies' proposed solution integrates the core SSI building blocks of decentralized IDs, decentralized storage, verifiable credentials, and cryptocurrency into a unified framework upon which interoperable applications can be built. Control over personal data is returned to the individual, ensuring safety and security while facilitating the sharing of permissioned, authenticated, high-quality data between individuals and trusted entities.

IV. Solutions: Self-Sovereign Identity

Definition of Self-Sovereign Identity

Self-sovereign identity (SSI) is an approach to digital identity that gives individuals direct control over the information they use to prove who they are to websites, services, and applications across the web. SSI is a decentralized system that allows individuals to securely and privately manage their personal identity data, maintaining ownership, control, and portability without relying on intermediaries. By creating and managing their own digital identities, users can securely access digital services, verify their identity, and share personal information selectively and on their own terms.[16]

---

[14] Straits Research. (2025). *Self-sovereign identity (SSI) market trends, key players, and growth opportunities 2025.* https://straitsresearch.com/report/self-sovereign-identity-market; KYCHub. (2025). *Self-sovereign identity (SSI): A complete guide for 2025.* https://www.kychub.com/blog/self-sovereign-identity/

[15] StationX. (2026). Biggest data breaches in history. StationX. https://app.stationx.net/articles/biggest-data-breaches; DeepStrike. (2026). Data breach statistics 2025–2026: Global trends & costs. DeepStrike. https://deepstrike.io/blog/data-breach-statistics-2025

[16] Dock Labs. (2026). Self-sovereign identity: The ultimate guide 2026. https://www.dock.io/post/self-sovereign-identity

Unlike traditional identity management systems, SSI places the individual at the center of the identity model. SSI can be viewed as a human-centric data management paradigm where users own and control their identity and the personal data associated with it, storing it locally on their own devices or remotely on a distributed network, and selectively granting access to authorized third parties without the need for a trusted intermediary.[17]

This principle of sovereign identity extends beyond individuals. Other entities, including Internet of Things (IoT) devices and artificially intelligent (AI) agents, can similarly be assigned defined, verifiable digital identities. The integration of AI agents with SSI frameworks is transforming how individuals and organizations manage, secure, and leverage digital identities, enabling secure, user-centric identity systems built on blockchain technology. On FISE Technologies' SSI platform, AI and IoT data belong to an authenticated, accountable user. Decentralized ownership of AI and IoT data helps mitigate behavioral risks, establishes trust and accountability, and creates measurable improvement metrics for owners and controllers of AI agents and IoT devices.[18]

Key Features and Benefits of SSI by FISE Technologies

In traditional identity management systems, users rely on third parties such as government agencies or social media platforms to store and manage their identity data, creating persistent exposure to identity theft, data breaches, and systemic privacy violations.

The dialogue about what self-sovereign identity truly means, begun by Christopher Allen's 2016 blog post "The Path to Self-Sovereign Identity," has not resulted in a universal consensus. While some regard Allen's ten principles as the definitive framework for SSI, he formulated them as a departure point to provoke discussion about what is truly important. SSI solutions are broadly understood to adhere to the following principles: existence, control, access, transparency, persistence, portability, interoperability, consent, minimization, and protection.[19] These principles[20] are outlined below:

1. **Existence:** Users are able to create and manage their own digital identities without relying on a third party. This means that users are able to create their own unique identifiers, store their own identity data, and control who has access to their data.
2. **Control:** Users have complete control over their digital identities and personal data. Users create, modify, and delete their own data. They are in control of managing it. Also, users are able to decide who has access to their data, and they are able to revoke access at any time.

[17] Mühle, A., et al. (2018). As cited in: Arxiv. (2021). Towards a trustful digital world: Exploring self-sovereign identity ecosystems. https://arxiv.org/pdf/2105.15131
[18] Chaffer, T. J., & Goldston, J. (2022). As cited in: Arxiv. (2024, December). Incentivized symbiosis: A paradigm for human-agent coevolution. https://arxiv.org/pdf/2412.06855
[19] Allen, C. (2016). The path to self-sovereign identity. Life with Alacrity. As cited in: eSSIF-Lab. (2024). Self-sovereign identity (SSI). https://essif-lab.github.io/framework/docs/terms/self-sovereign-identity/
[20] Agrawal, R. (2019, April 5). Self-sovereign identity: 10 guiding principles. LinkedIn. https://www.linkedin.com/pulse/self-sovereign-identity-10-guiding-principles-ravikant-agrawal

3. **Access:** Users are able to easily access their own data at any time without having to go through a third party.
4. **Transparency:** The processes and algorithms used to manage and update an identity system are transparent and understandable to users. Users easily understand how their data is being used, and they are able to make informed decisions about who has access to it.
5. **Persistence:** Identities possess durability and persistence. Users employ their digital identity over extended periods without concerns about invalidation or obsolescence. These identities are intentionally designed to withstand the evolving digital landscape.
6. **Portability:** Identities are seamlessly transferred across diverse systems and networks. Users employ their digital identity across multiple services and applications, eliminating the need to create a new identity for each platform.
7. **Interoperability:** Digital identities are readily accessible and usable for all users. They are employed with various organizations, eliminating the need for repetitive and time-consuming verification procedures.
8. **Consent:** Users have the right to control their data. Users decide who has access to their data, and they may revoke access at any time. Users do not have to give their data away without their consent.
9. **Least Disclosure:** Digital identity solutions enable users to share only the necessary data. Users are solely required to share the specific data pertinent to a particular transaction, without the need to disclose any additional information.
10. **Protection:** Data remains safeguarded against unauthorized access and interception. Users have the option to encrypt their data to prevent unauthorized parties from reading it. The authorized user retains control over the encryption process.[21]

V. Framework Architecture and Technical Details

For a self-sovereign identity system to be functionally secure, safe, and accessible, it must provide mechanisms to manage decentralized identities, decentralized storage, verifiable credentials, and a wallet for currencies used in financial transactions. FISE Technologies' platform, Signet, transfers ownership and control of personal data back to the individual, empowering users to manage their digital identities, credentials, and data assets from a single unified interface. The framework provides the mechanisms for users to create, manage, and potentially monetize a comprehensive personal data portfolio.

Decentralized Identities

Decentralized identity refers to an identity model in which individuals hold direct ownership and control over their own identity data, rather than relying on centralized authorities or third-

[21] Metadium. (2021, December 9). *Self-sovereign identity principle #10: Protection.* Medium. https://medium.com/metadium/self-sovereign-identity-principle-10-protection-305eb3068702

party intermediaries to manage, verify, or govern it. In a decentralized identity system, individuals create and manage their own digital identities, anchored in verifiable claims about their attributes and credentials — including name, address, date of birth, or educational and professional qualifications.

Decentralized identity delivers significant advantages over traditional approaches, including substantially increased privacy and security, reduced risk of identity fraud and unauthorized access, secured and consent-based access to verifiable services and resources, and meaningful, enforceable ownership and control over personal data. Together, these benefits establish decentralized identity as the foundational building block of a user-sovereign digital future.

Decentralized Storage

Decentralized storage is a method of storing data across a distributed network of nodes rather than in a centralized location managed by one or more custodial corporations or institutions. This architecture provides significant advantages over traditional centralized storage, including:

- **Greater Security**: Decentralized storage substantially increases the complexity for attackers attempting to access or exfiltrate data, as they must simultaneously compromise multiple independent nodes across the network rather than a single point of failure.
- **Increased Privacy**: Users retain direct control over their stored data, including the ability to determine who has access to it, under what conditions, and for how long, without deferring those decisions to a corporate custodian.
- **Improved Resilience**: Because data is distributed across multiple nodes rather than housed in a single location, decentralized storage is inherently more resilient to outages, infrastructure failures, and targeted attacks.
- **Reduced Costs**: Decentralized storage can be significantly more cost-effective than centralized alternatives, as pricing is governed by broader market availability and competition among storage providers rather than by monopolistic or oligopolistic custodial pricing.[22]

Verifiable Credentials

Verifiable credentials are a form of cryptographically secured digital credential that empowers individuals to securely and reliably share personal information with organizations and other parties without reliance on a central authority for verification. Credentials are generated using decentralized services and undergo cryptographic verification to guarantee their integrity and prevent unauthorized tampering or falsification.

[22] Acceldata. (2025, May 19). *Decentralized data storage: Security, privacy, and ownership.* https://www.acceldata.io/blog/decentralized-data-storage-future-of-secure-cloud-solutions

The "Triangle of Trust" represents the foundational relationship between three roles in the verifiable credentials ecosystem, enabling secure, privacy-preserving digital identity verification:

- **Issuer**: Responsible for generating and issuing verifiable credentials to holders, ensuring their validity and integrity through cryptographic digital signatures that bind the credential to its subject and attest to its authenticity.
- **Holder**: Possesses and controls their own verifiable credentials, storing them securely in a digital wallet. The holder selectively shares credentials based on specific transactional needs, retaining full ownership of their personal information at all times and disclosing only what is necessary.
- **Verifier**: Relies on a network of trusted issuers and advanced cryptographic techniques to validate the authenticity and integrity of presented verifiable credentials, independently confirming the claims made by the holder without requiring direct communication with the issuing authority.[23]

Cryptocurrency Wallets

Cryptocurrency wallets are secure software applications designed to facilitate the storage, management, and transfer of digital assets including Bitcoin, Ethereum, and a broad and growing ecosystem of cryptocurrencies and tokenized assets. These wallets employ advanced cryptographic techniques to generate public and private key pairs, which are used to securely authorize and execute the sending and receiving of digital currencies across various blockchain networks.[24]

Wallets are essential instruments for managing digital asset holdings, executing peer-to-peer transactions, and maintaining real-time visibility into balances and transaction history. They provide users with direct, self-custodied control over their digital assets — including cryptocurrencies, non-fungible tokens (NFTs), and other tokenized holdings — without dependence on a financial intermediary or custodial third party.

Within FISE Technologies' Signet platform, the cryptocurrency wallet is fully integrated into the user's identity and data portfolio, meaning digital assets are managed alongside credentials, decentralized IDs, and personal data from a single unified interface. The wallet incorporates layered security features including two-factor authentication, cryptographic key management, and user-controlled access permissions, ensuring that unauthorized parties cannot access or transfer a user's digital assets under any circumstances.

This integration of financial sovereignty with identity sovereignty represents a defining feature of the Signet platform and a meaningful advancement over standalone wallet solutions that operate in isolation from a user's broader digital identity ecosystem.

---

[23] *Sporny, M., Longley, D., Sabadello, M., Reed, D., Steele, O., & Allen, C. (2025, May 15). Verifiable credentials data model v2.0. World Wide Web Consortium (W3C). https://www.w3.org/TR/vc-data-model/*

[24] *Ledger. (2025, June 20). What is a crypto wallet? Ledger. https://www.ledger.com/what-is-a-crypto-wallet*

VI. Core Components of the FISE Technologies Framework

Decentralized Identifiers (DIDs)

Upon new account registration on the Signet platform, a cryptographically generated decentralized identifier (DID) is automatically assigned to the user. DID assignment occurs seamlessly in the background and is fully transparent to the user, remaining visible and accessible within the user interface at all times. All DIDs on the Signet platform conform to the W3C Decentralized Identifiers (DIDs) v1.0 specification, ensuring interoperability with the broader decentralized identity ecosystem.[25]

A decentralized identifier is a Uniform Resource Identifier (URI) composed of three distinct parts:

- **Scheme**: The first component of a DID, identifying it as a decentralized identifier. The current globally recognized standard uses the did: scheme, distinguishing decentralized identifiers from other URI types and signaling compatibility with W3C-compliant DID resolution infrastructure.
- **Method**: The second component of a DID, specifying the mechanism by which the DID was created, registered, and resolved. The method defines how the DID Document associated with the identifier is read, written, and updated on the underlying distributed ledger or decentralized network. Examples include the DID Method Resolution Service (DMR) and the Verifiable Credential Data Model (VCD).
- **Identifier**: The third and final component of a DID, constituting a globally unique string that unambiguously identifies the specific individual, entity, device, or object to which the DID is assigned. No two identifiers within a given DID method are alike, ensuring the integrity and uniqueness of every identity on the network.

Syntax example:

```
did:exampleMethod:123abc456def7890z
```

DID subjects, controllers, and documents

The subject of a DID is the entity identified by the identifier, which may be a person, group, organization, physical object, or abstract concept. The controller of a DID is the entity that holds the cryptographic authority to make changes to its associated DID Document, with that authority governed and enforced by a set of cryptographic keys held exclusively by the controller.

[25] *World Wide Web Consortium (W3C). (2026, March 5). Decentralized identifiers (DIDs) v1.1. W3C Candidate Recommendation Snapshot. https://www.w3.org/TR/did-1.1/*

DID Documents contain the information associated with a given DID, including cryptographic public keys used for authentication and verification, and interactive service endpoints relevant to the DID subject. Together, these elements enable trustworthy, tamper-evident interactions with the subject across decentralized networks.

A verifiable data registry is the underlying system responsible for recording DIDs and returning the data necessary to produce and resolve DID Documents. Examples include distributed ledgers, decentralized file systems, and peer-to-peer networks, each providing a transparent, censorship-resistant foundation upon which decentralized identity can be established, maintained, and verified without reliance on a central authority.

Decentralized Storage

The main architectural components of FISE Technologies' decentralized storage implementation include three stable and secure layers:

- **Public Network**: Composed of a large number of nodes connected to the internet as peers and geographically distributed across the world, the public network provides the foundation for resilient, censorship-resistant data storage. Users' data is stored across these nodes in file pieces linked by a directed acyclic graph (DAG), a structure that ensures data integrity and efficient retrieval. File pieces are duplicated across multiple nodes for redundancy, protecting against data loss in the event of individual node failure. Users may store both encrypted and unencrypted data, and all data may be digitally signed to establish provenance and verify authenticity.
- **Private Network**: A highly controlled, permissioned data network accessible exclusively by authorized users and entities. The private network temporarily stores data that is actively shared between parties during a transaction or interaction, ensuring that sensitive information remains confined to its intended recipients throughout the exchange and is never exposed to the broader public network.
- **Storage Broker Service**: The storage broker service acts as the intelligent intermediary between the user and the decentralized storage network, managing all read and write operations to and from decentralized nodes. It generates a cryptographic hash of each data object to produce a unique, tamper-evident identifier used for pinning and naming, and handles the linking of related data objects to solidify and enforce relationship definitions across the broader data portfolio.

Verifiable Credentials Infrastructure

The credential infrastructure is a decentralized protocol for issuing, presenting, and verifying verifiable credentials (VCs). VCs are cryptographically secured digital certificates that represent authenticated claims about an individual, organization, or entity. The infrastructure is architected to be secure, privacy-preserving, and scalable across a broad range of use cases and industries.

The credential architecture is organized into three distinct layers:

- **Application Layer**: The application layer is where user-facing applications interact with the Signet platform to create and manage credentials. It exposes a set of developer APIs that allow applications to generate, manage, rotate, and utilize cryptographic keys, enabling seamless integration of credential functionality into third-party decentralized applications (DApps) built on the FISE framework.
- **Network Layer**: The network layer is responsible for the reliable transfer of key events between nodes using a peer-to-peer communication protocol. By distributing event propagation across the network rather than routing through a central server, this layer ensures that credential events are delivered consistently, resiliently, and without dependence on any single point of failure.
- **Storage Layer**: The storage layer is responsible for the durable, tamper-evident persistence of credential events using the decentralized storage system described above. By distributing event storage across multiple nodes, this layer ensures that credential records remain resilient to targeted attacks, infrastructure failures, and unauthorized modification.

Overview of the Verifiable Credential Lifecycle:

1. **Request a Verifiable Credential**: The Holder initiates the process by creating a credential request and transmitting it to the Issuer. The request includes the Holder's DID, the type of verifiable credential being requested, and the specific claims the Holder seeks to assert about themselves.
2. **Issue a Verifiable Credential**: Upon receiving the credential request, the Issuer validates its contents and, if the request is determined to be legitimate, issues the VC to the Holder. The newly issued credential includes the Holder's DID, the verified claims, and the Issuer's cryptographic signature, which binds the credential to the issuing authority and renders it tamper-evident.
3. **Verifiable Presentation**: When access to a service or resource requires identity verification, the Holder presents the relevant VC to a Verifier. The Verifier independently evaluates the credential's authenticity and current validity using the Issuer's publicly available cryptographic key, without requiring direct communication with the Issuer.
4. **Verify a Verifiable Credential**: The Verifier cryptographically confirms the VC's authenticity by validating the Issuer's digital signature and may additionally cross-reference the credential's claims against the Holder's DID to ensure consistency, currency, and integrity before granting access or accepting the presented claims.

VII. User Stories

Examples of how the FISE Technologies' SSI framework can be used in various domains:

Neurodata Sovereignty and Brain-Computer Interface (BCI) Data Rights

Morgan has been using a brain-computer interface (BCI) device to assist with focus, cognitive performance monitoring, and early detection of neurological stress patterns. The device generates a continuous stream of neural data including thought patterns, cognitive states, and motor intentions representing some of the most intimate and sensitive data a human being can produce. Until now, that data has belonged entirely to the device manufacturer, stored on proprietary servers with no transparency into who accesses it, how long it is retained, or whether it is shared with third parties.

Through the FISE platform, Morgan receives a master decentralized identifier (DID) that governs the retrieval of the neurodata from their BCI device, including all neural data streams, and any AI agents (from Signet) operating on their behalf. Once retrieved and encrypted/stored into their Signet account, the neural data records are cryptographically anchored to their sovereign identity, creating verifiable, tamper-evident provenance that establishes Morgan as the legal and economic owner and controller of that data.

When a neuroscience research institution requests access to Morgan's anonymized neural data for a longitudinal cognitive health study, Morgan's AI agent reviews the proposed terms, confirms the data use is within Morgan's explicitly permitted parameters, and executes a smart contract governing the transaction. Seventy percent of the data sale revenue flows automatically and directly into Morgan's cryptocurrency wallet, with enforceable terms that make any unauthorized use of the data outside the agreed scope a legally actionable violation, with FISE Technologies standing as co-plaintiff to enforce Morgan's data rights.

Within Signet, Morgan retains full visibility into the complete audit history of who has accessed their neural data, under what terms, and for what purpose, a level of transparency that has never previously existed for BCI and neurotech users. Data shared or monetized through the Signet platform is governed by executed smart contracts that define the precise duration, scope, and permitted use of access. Any use of that data outside the agreed contractual terms constitutes a legally enforceable violation, with FISE Technologies standing as co-plaintiff to enforce Morgan's data rights. Morgan's sovereign identity and data portfolio, as maintained within the Signet platform, remain portable across compatible devices, platforms, and healthcare providers, ensuring that Morgan’s ownership of their Signet-registered data does not transfer to any institution, manufacturer, or intermediary.

Digital Education Transcripts

The registrar at TechVerse University is responsible for maintaining the integrity, accuracy, and security of all academic records. The registrar champions an "extended transcript" concept that goes beyond traditional course grades to encompass a comprehensive record of learner competencies, including academic achievements, relevant work experience, and marketable skills developed outside the classroom. At the request of students, the registrar issues a digital verifiable credential incorporating the extended transcript, providing employers, institutions, and other verifying parties with a complete, tamper-evident, and instantly verifiable representation of each student's qualifications.

Finance KYC Use/Reuse

Alex wants to open a bank account. As part of the Know Your Customer (KYC) verification process, the bank requests that she confirm her identity. Alex selects government-issued verifiable credentials that authenticate her residence and citizenship and presents them directly from her Signet wallet. The bank verifies the credentials cryptographically and opens her account, then issues Alex a new credential that she can use to securely authorize future account transactions. Alex can reuse the same government-issued verifiable credentials to open accounts at additional financial institutions, eliminating the need to submit the same identity documentation repeatedly and reducing friction across the financial services ecosystem.

Purchases Requiring Proof of Age

Riley visits Tipsy Taps liquor store to purchase a bottle of wine. Rather than presenting a physical ID, Riley presents a verifiable identity credential from their Signet wallet. The credential allows the liquor store owner to cryptographically confirm that Riley meets the legal drinking age requirement without disclosing their actual date of birth, home address, gender, or state ID number. Only the minimum necessary information is shared, preserving Riley's privacy while fully satisfying the retailer's legal verification obligation.

Data Monetization

Jordan, a Signet platform user, seeks financial compensation for sharing their demographic information with research organizations. Through granular, explicit permission settings within the platform, Jordan specifies that anonymized personal demographic data may be made available exclusively to organizations conducting approved academic or market research. All data shared under these permissions is fully anonymized prior to release, preventing any direct association with Jordan's identity. Payments made by organizations accessing the data are distributed back to contributing platform users, with a designated portion deposited directly into Jordan's cryptocurrency wallet.

Facilitation of Job Placement

FictiveSoft has posted an open position online and is receiving thousands of applications. Unlike the majority of applicants, Jamie has attached education credentials issued by recognized, verified credential issuers directly to their application. FictiveSoft's applicant tracking system evaluates these credentials automatically upon receipt, verifying their authenticity and integrity in real time without manual review. Because Jamie's materials are cryptographically verifiable and instantly confirmed, their application is immediately surfaced and forwarded as a viable candidate, giving Jamie a decisive advantage in a competitive applicant pool.

Health Diagnostic Support

Rather than having a fragmented subset of personal medical information siloed across numerous healthcare providers, a Signet user maintains a unified, comprehensive medical record accessible in its entirety from their identity portfolio. When engaging with a healthcare provider, the user shares only the specific information required for the encounter, transmitted securely and with explicit consent. Access can be revoked at any time, returning full control to the individual. The platform also supports user-orchestrated data analytics on personal health information, enabling proactive tracking of health conditions, identification of trends, and generation of personalized health recommendations, all under the user's direct governance.

Proof of AI Bot Legitimacy

As AI agents become increasingly integrated into daily decision-making, establishing the credibility and provenance of those agents is essential. Jamie seeks an AI medical agent to serve as a collaborative tool for symptom diagnosis. By querying the Signet platform for AI agents whose credentials are cryptographically tied to renowned health institutions including Johns Hopkins, Mayo Clinic, Columbia University, and UC San Francisco, Jamie identifies the most reputable and verified agent from which to seek medical guidance. This credential-based model of AI accountability ensures that all digitally produced content and recommendations are appropriately attributed to a trusted, verifiable source.

VIII. Challenges and Limitations

Slowness of Decentralized Systems

Critics have noted that reliance on decentralized technologies in SSI systems can result in reduced speed and efficiency compared to traditional centralized systems, due to the distribution of processing across numerous nodes, which may introduce latency. By 2025, however, Layer 2 scaling solutions have matured into production-grade infrastructure, with rollups, particularly optimistic rollups and zero-knowledge rollups, bundling large numbers of transactions to dramatically increase throughput while reducing fees and latency. Complementary technologies including IPFS swarm connections and Content Delivery Networks (CDNs) further reduce latency and improve performance at the application layer. The benefits of increased security, privacy, and user control over personal data continue to outweigh the performance trade-offs, and the gap between decentralized and centralized system performance is narrowing rapidly as the ecosystem matures.[26]

[26] LCX. (2025, December 15). *Blockchain scalability in 2025: Are we finally solving the throughput problem?* https://www.lcx.com/blockchain-scalability-in-2025-are-we-finally-solving-the-throughput-problem/

Reliance on Verifiable Credentials (VCs)

The reliance on verifiable credentials presupposes that credential issuers are trustworthy and reliable, which may not always be the case, and establishing a universally accepted standard for verifiable credentials across jurisdictions and industries remains an ongoing challenge. The Signet platform addresses this by standardizing the foundational processes critical to baseline SSI functionality, conforming to the W3C Verifiable Credentials Data Model v2.0 as the governing standard. Verifiable credentials issued through the platform are cryptographically signed, encrypted, and stored on a decentralized network of nodes, making it computationally impractical for malicious actors to tamper with or forge them.[27]

Perception of Cryptocurrencies

Cryptocurrencies have faced criticism for market volatility, an evolving regulatory landscape, and historical associations with illicit activity. Security concerns, volatility, and regulatory oversight continue to represent barriers to broader adoption, though values of major cryptocurrencies including Bitcoin, Ethereum, Ripple, and Solana reached historic record highs over the course of 2025, and capital inflow from institutional Wall Street ETFs provided significant support for price stability. The EU's Markets in Crypto-Assets (MiCA) regulation became fully operational in December 2024, introducing a structured compliance framework across member states, and the U.S. has shifted toward a more defined federal posture on digital assets. As the regulatory environment matures and institutional adoption accelerates, the role of cryptocurrency in self-sovereign identity systems, providing greater security, privacy, and user-controlled financial transactions, is increasingly well-supported.[28]

Ease of Use

Many of the technologies underlying a self-sovereign identity system remain unfamiliar to the average internet user, and complexity of use continues to represent a meaningful barrier to entry and mass adoption. FISE Technologies addresses this directly through the following thoughtful UI design principles embedded in the Signet platform:

- **Step-by-Step Instructions**: Wizard-based guided flows walk users through obtaining verifiable credentials, adding them to their SSI portfolio, and sharing them with third parties — reducing friction at every stage of the credential lifecycle.
- **Clear and Concise Language**: The user interface is deliberately free of technical jargon, presenting complex cryptographic and decentralized identity concepts in plain, accessible language appropriate for users at all levels of technical familiarity.

[27] Sporny, M., Longley, D., Sabadello, M., Reed, D., Steele, O., & Allen, C. (2025, May 15). Verifiable credentials data model v2.0. World Wide Web Consortium (W3C). https://www.w3.org/TR/vc-data-model/

[28] Security.org. (2026, May 11). 2026 cryptocurrency adoption and sentiment report. https://www.security.org/digital-security/cryptocurrency-annual-consumer-report/; CoinLaw. (2025). Cryptocurrency trading regulations statistics 2025. https://coinlaw.io/cryptocurrency-trading-regulations-statistics/

- **Progressive Disclosure**: Additional information, options, and controls are revealed incrementally as users need them, reducing cognitive load and preventing the interface from overwhelming new users during onboarding.
- **Familiar Concepts**: File system management paradigms are employed to represent data the user owns in decentralized storage, making the experience intuitive for anyone familiar with organizing files on a computer. An address book interface manages all user-validated entities, providing a recognizable mental model for identity and contact management within the platform.

IX. Advantages and Benefits

Selective Disclosure with Verifiable Credentials

In today's predominant identity systems, sharing personal information with a requesting party typically requires handing over far more Personally Identifiable Information (PII) than the transaction actually requires. Centralized and federated identity systems force users to overshare information, resulting in personal data being copied, stored, sold, breached, and shared far beyond user expectations. The Signet platform resolves this through selective disclosure; users manage their issued verifiable credentials and select only the specific attributes within a credential required for a given transaction, sharing nothing more with the Verifier. Holders of verifiable credentials can provide to verifiers a subset of a credential, enabling selective disclosure of private data, or combine several credentials into a single verifiable presentation where short-lived proofs are not intended to be stored for extended periods. The Verifier receives only what is necessary and retains no duplicate copy of the user's underlying credential data.[29]

Decentralized Datastores

The Signet platform utilizes decentralized storage to directly address the structural limitations of centralized databases. Rather than confining data to a single server owned and managed by a corporate custodian, data is distributed across a network of independently operated nodes. All data stored across these nodes is encrypted at rest, substantially increasing the difficulty for malicious actors to compromise and extract meaningful information from any individual node. Decentralized storage provides a more secure, cost-efficient, and resilient alternative by distributing data across multiple nodes, ensuring that users retain control over their information at all times, without delegating that control to a third-party institution.[30]

---

[29] Walt.id. (2026, March 16). Selective disclosure. https://docs.walt.id/concepts/selective-disclosure; W3C. (2025, May 15). W3C publishes verifiable credentials 2.0 as a W3C standard. https://www.w3.org/press-releases/2025/verifiable-credentials-2-0/

[30] Acceldata. (2025, May 19). *Decentralized data storage: Security, privacy, and ownership.* https://www.acceldata.io/blog/decentralized-data-storage-future-of-secure-cloud-solutions

Users are in Control of Their Own Identity

With the Signet platform, current identity providers are no longer required to store individuals' personal information on their behalf. Signet's Decentralized Identifiers (DIDs) are anchored on peered nodes within decentralized storage, ensuring the persistence of identity information and the reliability of access regardless of the status of any individual node or service provider. Users can create and manage multiple distinct identities within the platform, enabling them to share different facets of a whole identity in different contexts such as presenting a professional identity to an employer, a patient identity to a healthcare provider, and a financial identity to a bank, all from a single sovereign identity portfolio.

Privacy Improves

The Signet platform automates encryption, digital signatures, and decentralized storage as default behaviors, delivering meaningfully better baseline privacy than non-SSI, centralized web-based systems where these protections must be deliberately sought out and are rarely guaranteed. Through data encryption for confidentiality, digital signatures for integrity and provenance, decentralized storage for resilience against attack and institutional failure, and individual control over all data sharing decisions, the Signet platform ensures that personal information remains secure, private, and under the sole governance of the individual user, not the platform, not the institution, and not the network.

X. Deployment

The Signet platform will initially be deployed as a web-based front-end, providing a platform-independent implementation accessible to clients on any device supporting a modern web browser, across all major operating systems including Android, Apple iOS, Microsoft Windows, macOS, and Linux. This approach ensures broad accessibility from day one, requiring no proprietary software installation and enabling users to engage with the full platform from desktop, tablet, or mobile devices without friction.

Upon creating an account, each user is automatically assigned a unique decentralized identifier (DID) along with a corresponding cryptographic key pair. These keys serve as the foundation for the user's sovereign identity on the platform, enabling identification, data encryption, private data sharing, and functioning as the user's primary identifier against which all subsequent verifiable credentials are anchored. The key assignment process occurs seamlessly in the background and is transparent to the user through the Signet interface.

Decentralized storage is deployed across a distributed network of existing public and private peered nodes, utilizing libp2p protocols to discover, connect to, and store data files across the network. This peer-to-peer networking layer ensures that data retrieval and storage operations are resilient, performant, and free from dependence on any single infrastructure provider or custodial server.

Following account creation, each user is issued a non-custodial cryptocurrency wallet with a unique wallet address defined on the Ethereum blockchain. Non-custodial issuance ensures that the user, and only the user, holds the private keys governing their digital assets at all times. From Signet's client-side interface, all standard wallet functions are available, including sending and receiving cryptocurrency, storing digital assets, viewing real-time balances, and encrypting and digitally signing transactions, providing users with full financial sovereignty within a single unified platform.

XI. Roadmap and Future Work

Once the core capabilities of the Signet platform have been solidified and validated, future development efforts will concentrate on the seamless integration of self-sovereign identity applications, including decentralized applications (DApps) built natively on the Signet framework. Expanding the ecosystem of available SSI applications will enable users to engage with an increasingly broad and interconnected suite of identity-driven services from within a single sovereign platform. Additional integrations will include verifiable credential issuers interacting directly through the Signet enterprise platform, concurrent with the implementation of advanced platform capabilities such as comprehensive audit trails, enhanced compliance tooling, and expanded credential lifecycle management.

To ensure long-term platform stability, scalability, and decentralization, FISE Technologies actively fosters collaboration with organizations whose core infrastructure and development activities support and extend the Signet platform's decentralized processes. These partnerships strengthen the underlying network upon which Signet operates and contribute to the resilience and robustness of the broader SSI ecosystem.

FISE Technologies additionally pursues strategic and synergistic collaboration with organizations interested in building SSI applications and DApps on the Signet platform, aiming to continuously expand the repertoire of available SSI capabilities accessible to users. By cultivating a developer and enterprise partner ecosystem around the Signet framework, FISE Technologies positions the platform as the foundational infrastructure layer upon which the next generation of user-sovereign digital applications is built.

XII. Conclusion

Self-sovereign identity (SSI) represents a transformative shift in how individuals relate to their personal data, their digital identities, and their financial lives. It provides the mechanisms for individuals to retain full, verifiable ownership over their personal information while establishing provable, cryptographically enforceable trust between parties across a wide range of digital interactions. Building a robust and scalable SSI ecosystem requires four foundational pillars, each of which is fully realized within the Signet platform:

- **Decentralized Storage**: Enables users to securely store personal data across a distributed network of nodes rather than on a single server controlled by a corporate

custodian, making it significantly more difficult for unauthorized parties to access, control, modify, or delete that data without the user's explicit consent.

- **Decentralized Identifiers (DIDs)**: Give users direct, sovereign control over their own identity information, including the ability to determine what is shared, with whom, under what conditions, and for how long, without delegating those decisions to a centralized identity provider.
- **Verifiable Credentials**: Enable users to share identity information with third parties in a cryptographically secure and instantly verifiable manner, providing receiving parties with confidence that the information presented is accurate, untampered, and attributable to the correct individual or entity.
- **Cryptocurrency Interoperability**: Allows users to transact for goods and services without exposing sensitive personally identifiable information connected to traditional banking or credit card systems, with the integrated non-custodial wallet protecting user privacy, financial sovereignty, and transactional security.

The FISE Technologies platform, Signet, as presented in this white paper, represents a foundational and innovative advancement in the practical adoption of self-sovereign identity at scale. By unifying these four pillars into a single, cohesive, and interoperable framework, Signet lowers the barrier to SSI adoption for individuals, developers, enterprises, and institutions alike. Its comprehensive support for SSI applications, verifiable credential infrastructure, decentralized storage, and sovereign financial tooling positions it as the infrastructure layer upon which the next generation of user-sovereign digital experiences can be built.

FISE Technologies is committed to building a secure, decentralized, and accessible SSI system that returns meaningful control of personal data and finances to the individual; implementing the architectural pillars, technical standards, and design principles described throughout this white paper, and advancing a future in which human data sovereignty is not an aspiration but a provable, enforceable reality.
