INATBA REPORT

Building Trust: Integrating AI, Blockchain, and Digital Identity

November 2025

INATBA

International Association
for Trusted Blockchain Applications

Authors

Åsa Dahlborn, BlackVogel, Germany

Catarina Ferreira da Silva, EU Blockchain Observatory and Forum, Portugal

Fabio Budris, ID LATAM Forum, AI & Blockchain Convergences Task Force Co-Chair, Argentina

Horst Treiblmaier, Modul University Vienna, INATBA Academic Advisory Board, Austria

Ingrid Vasiliu-Feltes, EU Blockchain Observatory and Forum, United States of America

Jim Mason, EU Blockchain Observatory and Forum, United States of America

Jolanda ter Maten, EU Blockchain Observatory and Forum, the Netherlands

Lynn Chia, Modul University Vienna, Singapore

Maarten Boender, 4Sure Technology Solutions, the Netherlands

Mariana de la Roche, BlackVogel, thinkBLOCKtank, AI & Blockchain Convergences Task Force Co-Chair, Germany

Paolo Giudici, University of Pavia, INATBA Academic Advisory Board, Italy

Tomaz Sedej, LF Decentralized Trust, United States of America

Reviewers

Inon Schenker, Tel Aviv University, INATBA Academic Advisory Board, Israel

Mat Yarger, Demia, United States of America

Professor Joyce O'Connor, BlockW, INATBA Academic Advisory Board, Ireland

Table of Contents

1. Executive Summary

The convergence of Self-Sovereign Identity (SSI) and Artificial Intelligence (AI) represents a significant step toward establishing a global benchmark for digital trust, rights-based governance, and competitiveness.

Key Messages

- SSI as a Trust Anchor: SSI restores control over identity to citizens and organizations, reducing dependency on centralized intermediaries and opaque data brokers.
- AI as a driver of Intelligence and Automation: When trained on verifiable and provenance-rich data, AI improves risk detection, compliance, and decision-making at scale.
- Synergy: Together, SSI and AI form systems that are transparent, auditable, and human-centric, supporting resilience against fraud, identity manipulation, and systemic bias.
- Regulatory Alignment: The combined framework directly supports compliance with the GDPR, eIDAS 2.0, and the EU AI Act, while reinforcing the goals of the Digital Services Act, Digital Markets Act, Cyber Resilience Act, Data Governance Act, and Data Act.
- Societal Impact: Beyond technical gains, SSI + AI address critical challenges such as digital inclusion, accountability of autonomous agents, and protection against synthetic identities, enabling the safeguarding of democracy, empowering citizens, and unlocking economic opportunities.

Strategic Relevance

In a digital economy where identity defines access to finance, healthcare, education, and civic rights, the convergence of SSI and AI is not optional — it is foundational. Europe has the regulatory leadership, technological infrastructure, and governance culture to set global standards. This report offers a roadmap to operationalize this leadership.

2. Introduction

2.1. Context: Evolution of Digital Identity

Digital identity has evolved from basic login and federated models (early 2000s) to identity as critical infrastructure (mid-2010s) to SSI as a paradigm of user-controlled, verifiable trust (post-2015). This transition reflects growing needs for privacy, inclusion, and rights-based governance.

The earliest phase of digital identity was marked by simple username–password mechanisms and the first federated systems, where large platforms such as Google or Facebook acted as central authenticators. While convenient, these models concentrated power and data in the hands of a few providers, raising concerns over surveillance, data breaches, and loss of user agency.

The second phase, beginning in the mid-2010s, positioned identity as a form of critical infrastructure. Governments, enterprises, and service providers began to integrate identity solutions into financial services, healthcare, and public administration. Identity became more than a credential for access: it became the backbone of trust for digital economies. However, this model still relied heavily on centralized databases and third-party verification, which limited portability, created vendor lock-in, and introduced systemic risks.

The third phase, emerging after 2015, is the rise of Self-Sovereign Identity (SSI). Unlike earlier approaches, SSI enables individuals and organizations to control their own verifiable credentials, share them selectively, and prove claims without relying on a central authority. It introduces cryptographic assurance, interoperability across ecosystems, and privacy-preserving mechanisms such as zero-knowledge proofs. This paradigm shift aligns digital identity with human rights principles, promoting autonomy, inclusion, and resilience against misuse.

This evolutionary trajectory also underscores the shifting balance between centralized trust and distributed trust. Each transition—first to federated models, then to identity as infrastructure, and now to SSI—represents not only a technological change but also a reconfiguration of power. Control over identity data moves gradually from institutions and corporations back to individuals. This redistribution of trust is critical in an era where digital interactions define access to services, participation in economies, and even civic rights. Moreover, the emergence of SSI coincides with broader socio-technical transformations: the acceleration of AI, the mainstreaming of blockchain, and the regulatory emphasis on data protection. Together, these dynamics reinforce the understanding that digital identity is no longer a peripheral tool—it is a foundational layer of modern society that underpins innovation, safeguards freedoms, and enables cross-border collaboration.

2.2. SSI and AI as Prerequisites for the Blockchain Ecosystem

Building on the foundation introduced by SSI, the next frontier of identity innovation framework and implementation involves its interaction with Artificial Intelligence (AI) systems. Identity is not only a credential but increasingly also a form of dynamic input for decision-making. Since AI systems are tasked with mediating credential verification, behavioral scoring, and eligibility determination in blockchain-native contexts, the integrity of identity inputs becomes vital. AI is fast becoming a crucial factor in shaping the usage, interpretation, and governance of identity in increasingly automated environments, which calls for more transparent, verifiable, and privacy-respecting data inputs for these systems to run ethically and reliably at scale.

SSI provides the infrastructure for anchoring such trust without relying on centralized authorities, and also helps to automate risk detection, credential validation, and fraud prevention in blockchain workflows. When trained on verifiable and provenance-rich identity data provided through SSI, these models can increase operational efficiency while mitigating bias and exclusion.

According to the INATBA AI & Blockchain Convergences Task Force, blockchain's immutability and consensus models offer "concrete mechanisms for embedding ethical principles in practice." SSI strengthens this by feeding AI systems with trustworthy, user-authorized inputs and enabling selective disclosure and verifiable audit trails.

For developers, regulators, and institutions building identity-aware AI within blockchain ecosystems, the integration of SSI also reduces reliance on opaque data brokers and unverifiable heuristics. Since SSI allows users to present cryptographically verifiable credentials directly from trusted issuers, this eliminates the need for data inference or third-party scoring. It facilitates alignment with regulatory principles such as purpose limitation, proportionality, and explainability by supporting selective disclosure and data minimization at the protocol level (World Economic Forum, 2018).

Self-Sovereign Identity (SSI) introduces new mechanisms across the data lifecycle:

- User-Centric Data Flow
- Verifiability of Claims
- No Silent Data Harvesting (operates on explicit disclosures instead of continuous background data collection).
- Selective Disclosure / Purpose-Bound Data Use

At a high level, SSI provides trusted and verified data about a person or entity, which AI then uses that data to make decisions or automate processes.

Blockchain ensures that all actions are recorded transparently and can't be tampered with. However, implementation challenges persist. These include managing cross-jurisdictional interoperability, reducing the latency of real-time credential validation, and addressing the computational overhead of privacy-enhancing mechanisms such as the INATBA AI & Blockchain Convergences Task Force.

To address these challenges, we need common technical standards that work across systems, faster and more efficient cryptographic tools, and governance frameworks that balance technology requirements with ethical and legal responsibilities. Recent regulatory and market developments have also demonstrated growing consensus on the need for private, safe, and accessible infrastructures. From the EU AI Act (2024/1689) to digital identity pilots in ASEAN, the African Union, and Latin America, governments and institutions are increasingly prioritizing approaches that place individuals, not platforms or centralized authorities, at the center of trust frameworks.

The integration of SSI and AI directly addresses long-standing challenges in established centralized identity systems, such as data silos, unverifiable claims, and limited user agency. While SSI enables individuals to hold and selectively share their own verifiable credentials, AI systems process that trusted data to automate decisions more efficiently and fairly. Together, SSI and AI can help to reduce risk, improve privacy, and support real-time decision-making in a fast and efficient way.

More importantly, they lay the foundation for identity systems that are not only secure and user-controlled but also equitable and accessible by design. In this emerging digital ecosystem, it is key that users have the autonomy and empowerment to participate in public and private domains without compromising their privacy, autonomy, or inclusion.

3. Theoretical and Conceptual Framework

3.1. Fundamentals of Self-Sovereign Identity (SSI)

Self-Sovereign Identity (SSI) is not just a technological upgrade to existing identity systems. It also represents a change in how identity is conceptualized, constructed, and governed in digital environments. Instead of just viewing identity as a static credential stored by centralized authorities, SSI frames it as a contextual, verifiable relationship that can be controlled by the individual. This shift also demands new competencies among citizens, professionals, and institutions, including the ability to apply selective disclosure and interpret cryptographic proofs in day-to-day interactions. This shift is important because it now repositions identity from being just an institutional asset into a

user-governed trust mechanism, which is also grounded in open standards, cryptographic verification, and decentralized governance models.

3.1.1. Definitions and Principles

Self-Sovereign Identity (SSI) refers to a user-centric approach to digital identity where an individual or entity is the main authority over their identity data. This is because SSI systems were designed to allow for secure, privacy-preserving interactions in both digital and physical environments. It relies on cryptographic mechanisms and open standards instead of institutional and/or centralized gatekeepers. To give a clearer illustration, there are three technical components at the core of SSI that enable decentralized trust and verifiable digital relationships:

Verifiable Credentials (VCs) are digitally signed statements issued by a trusted authority, such as universities, governmental bodies, or certifying bodies that are able to confirm specific and related information about a person or entity. These credentials are then stored and controlled by the holder and presented to third parties (verifiers) when proof is required. In this entire process, verification is fully done cryptographically, meaning that the authenticity of the credential can be validated without contacting the original issuer.

The three-part interaction model below summarises this interaction:

- Issuer: The entity that creates and signs the credential (e.g., a university issuing a diploma).
- Holder: The person and/or organization that stores and manages the credential.
- Verifier: The party requesting confirmation of the credential's validity.

This model facilitates data minimization by allowing the holder to share only necessary details when needed, such as proving age or citizenship, without disclosing other unrelated information.

Decentralized Identifiers (DIDs) are self-created, unique digital identifiers that are not tied to any central registry or service provider. Unlike traditional identifiers such as usernames, passport numbers, or platform-assigned IDs, DIDs are controlled entirely by the user and can be rotated, updated, or revoked without dependency on a third party. DIDs ensure trusted communication between parties by linking to cryptographic keys and publicly accessible metadata, often anchored on decentralized networks such as blockchains. This form of architecture allows identity systems to scale across domains without relying on platform monopolies or state-issued registries, meaning that DIDs maintain security and autonomy by enabling selective information disclosure about identity data across digital ecosystems.

Zero-Knowledge Proofs (ZKPs) are advanced cryptographic protocols that allow one party (the prover) to demonstrate to another party (the verifier) that a given statement is true without revealing any additional information beyond the validity of the statement itself. One example is proving that one is over 18 or possesses a valid license, all without revealing the underlying data. This supports selective disclosure, which is a key aspect of privacy-preserving identity systems. ZKPs enhance user agency by ensuring that sensitive attributes (e.g., full name, date of birth, address) do not need to be shared unnecessarily, to reduce data exposure and support compliance with regulatory principles such as proportionality and purpose limitation.

Together, technologies such as ZKPs, DIDs, and Verifiable Credentials embody a set of principles that help distinguish SSI from traditional identity systems, federated login systems, and/or opaque data brokers. Instead of viewing identity as a static credential administered by institutions, SSI treats it as a dynamic set of relationships and claims, anchored in verifiable trust but governed by the individual. In doing so, SSI provides a scalable, secure, and ethically aligned framework for identity in an increasingly decentralized and data-driven world.

3.1.2. Differences from Traditional Digital Identity Models

While traditional identity systems and models have helped establish the initial systems in scaling digital services during earlier phases of the internet, limitations became clearer when it came to addressing issues of user control, interoperability, data protection, and trust governance. In response to these limitations, SSI reimagines identity as a decentralized, user-governed framework underpinned by cryptographic assurance rather than institutional custody.

Single Points of Failure

In centralized systems, the identity infrastructure usually relies on one central authority or database to issue, store, and verify credentials. If that central system becomes unavailable, whether it is due to a technical failure, a cyberattack, or an administrative effort, all identity-related services dependent on it may be disrupted or compromised. This then creates a structural vulnerability because the failure of one node can compromise the entire system. For instance, if a national identity server goes offline, citizens may not be able to access banking services, healthcare, or e-government portals that depend on it.

Data Breaches

Since centralized identity systems often store large amounts of personal data in a single location, this aggregation can make it an attractive target for malicious actors. In the case of unauthorized access, mass exposure of sensitive information such as names, birthdates, social security numbers, and biometric data could be

leaked. Such an example of a high-profile breach of a national ID system was India's Aadhaar, where it exposed the personal data of millions due to vulnerabilities in centralized storage and access control.

Lack of User Visibility or Control

Users in centralized identity models usually also have limited insight in understanding how their data is being stored, shared, or used. Instead, decisions about data retention, access by third parties, or revocation of credentials are made by the central authority, which is often done without meaningful user consent or transparency. For example, a user may not be notified if their ID data is shared with law enforcement or third-party service providers, nor given an option to revoke that access.

Limited Portability Across Jurisdictions or Platforms

Identity credentials issued in centralized systems are often valid and usable only within the issuing institution or national framework. This lack of interoperability makes it difficult to reuse identity credentials across borders, sectors, or service platforms. This also means that different systems or different issuers/verifiers are required for a university login vs a national eID. One's credentials and identity data may not be usable for verifying identity with foreign institutions, online platforms, or decentralized services, forcing users to manage multiple credentials and verification processes across different platforms. This reflects the limitation of treating identity as a static attribute, rather than a dynamic, contextual interaction and relationship.

Federated Identity Systems

Federated identity systems, such as those based on SAML or OAuth protocols (e.g., "Login with Google" or "Login with Facebook"), allow users to access multiple online services using a single credential issued by a trusted provider. This model enhances convenience and reduces the burden of password management, but it also recentralizes control over digital identities in the hands of a few dominant technology platforms. Identity providers gain extensive access to behavioral data generated across authentication events, enabling them to profile, track, and monetize user activity—often beyond individuals' explicit awareness or consent. Such behavioral data may be exploited to infer sensitive personal attributes, including political preferences or psychological traits, thereby increasing the risks of surveillance, erosion of autonomy, and digital manipulation.

Moreover, federated identity models typically restrict interoperability to predefined ecosystems, reinforcing platform lock-in and constraining user sovereignty. The ability to revoke or suspend credentials often remains under the

provider's exclusive control, leaving users with little recourse, which underscores the systemic power asymmetries embedded in these architectures.

Platform-Based and Proprietary Models

Platform-specific identity systems such as Apple IDs, Amazon accounts, or even bank-issued digital IDs tend to anchor identity within closed commercial ecosystems. These systems are often non-interoperable, reinforcing vendor lock-in and creating data silos. They also rely heavily on opaque terms of service, shifting identity governance to private legal contracts rather than public standards or rights-based frameworks.

How SSI Differs Structurally

On a structural level, SSI differs from these models since it introduces a decentralized architecture, grounded in user agency, selective disclosure, and cryptographic trust. Rather than relying on real-time verification by central authorities, SSI enables verifiers to confirm credentials offline when issuer keys and current status information are locally available, based on the issuer's digital signature.

Below is a comparative overview:

Dimension	**Traditional Models**	**Self-Sovereign Identity (SSI)**
Control	Held by the issuing authority or platform	Held by the user
Identifiers	Assigned by provider (e.g., passport no., email, username)	Self-generated (DIDs)
Data Sharing	Broad, often automatic or inferred	Purpose-bound, explicitly consented
Verification	Requires institutional access (centralized validation)	Offline verification via digital signature
Interoperability	Platform-specific or siloed	Standards-based (e.g., W3C DID/VC)
Privacy Architecture	Surveillance-prone, metadata-rich	Privacy by design (selective disclosure, ZKPs)
Revocation	Controlled by the issuer	Governed by user or distributed governance models

In conclusion, SSI not only resolves longstanding technical limitations such as lack of interoperability and cross-domain credential reuse, but it also introduces a rights-based logic of identity, aligned with emerging regulatory instruments such as the General Data Protection Regulation (GDPR) and eIDAS 2.0. Importantly, SSI is not just technically distinct, but epistemologically and politically different because it shifts the locus of trust from institutional authority to protocol verifiability, and the governance of identity from private platforms to open, decentralized networks supported by international standards bodies such as the W3C and the Decentralized Identity Foundation (DIF).

While traditional identity systems define identity as a centralized assertion, SSI helps to reframe it as a dynamic, context-sensitive exchange mediated by cryptographic proofs and governed by shared protocols. This structural difference builds upon and complements existing systems, helping to shape a future where identity is not just digital, but dignified, interoperable, and user-controlled.

3.2. Fundamentals of Artificial Intelligence Applied to Identity

Artificial Intelligence (AI) is increasingly shaping the way digital identity systems are designed, managed, and governed. Within the context of SSI, AI provides the analytical and predictive capabilities required to process complex identity data at scale, while SSI ensures that such data is trustworthy, verifiable, and under the control of the user. The convergence of both technologies opens new pathways for secure, privacy-preserving, and user-centric identity ecosystems.

3.2.1. Relevant AI Techniques

Artificial Intelligence provides a broad set of techniques that can be applied to identity systems, each contributing distinct capabilities.

Machine learning enables the detection of patterns in large datasets, supporting tasks such as fraud detection, anomaly recognition, and behavioral risk scoring in identity verification.

Deep learning, with its ability to process unstructured data such as images, voice, or biometric signals, extends these applications to multimodal authentication and real-time verification at scale. However, the opacity of these models raises concerns in high-stakes environments like identity management.

For this reason, **Explainable AI (XAI)** has emerged as a critical complement, aiming to make decision-making processes transparent and interpretable to both regulators and end-users. By integrating XAI into SSI frameworks, systems can provide not only efficient and automated verification but also clear justifications for decisions, strengthening accountability, compliance, and user trust.

In practice, these AI techniques are already finding applications within SSI ecosystems. Machine learning models are being deployed to analyze credential usage patterns and detect anomalies that may indicate identity theft or replay attacks. Deep learning approaches enable biometric verification linked to verifiable credentials, such as facial or voice recognition, which, when combined with DIDs, strengthen multi-factor authentication without centralizing sensitive data. Meanwhile, XAI frameworks allow systems to explain why a credential was rejected—for example, clarifying whether a digital diploma failed due to an expired signature, an untrusted issuer, or an integrity breach. Such explanations are essential not only for building user confidence but also for regulatory compliance under frameworks such as the EU AI Act, which mandates transparency and auditability in AI-driven identity systems.

3.2.2. Data Protection, Biases, and Ethical Considerations

The integration of AI into identity management systems raises significant ethical challenges, particularly regarding data protection, bias, and accountability. While cryptographic mechanisms in SSI safeguard privacy and minimize unnecessary disclosure, the use of AI introduces risks of unintended profiling or discriminatory outcomes if models are trained on incomplete, biased, or non-representative data.

Mitigating bias is not merely a technical task; but it requires human oversight, interdisciplinary evaluation, and governance frameworks that ensure fairness and inclusivity. Ethical AI in the context of SSI demands transparency in how algorithms operate, clear lines of responsibility for decisions, and alignment with principles such as proportionality, purpose limitation, and informed consent.

Furthermore, explainability must extend beyond technical interpretability to practical communication, allowing users, regulators, and institutions to understand why identity-related decisions were made. In this sense, AI ethics within SSI ecosystems should be approached as a continuous process of monitoring, auditing, and refinement, rather than as a one-time compliance exercise.

More generally, Sustainability, Accuracy, Fairness and Explainability (S.A.F.E) AI applications should be encouraged by means of a consistent evaluation framework that can be used to assess their quality and to deliver AI models and agents that are S.A.F.E. by design.

3.2.3. Federated Learning & Confidential Computing

Traditional AI models often rely on centralized data aggregation, which is incompatible with the privacy-first principles of SSI. Federated learning offers an alternative by enabling AI models to be trained across multiple devices or institutions without centralizing raw data. Instead, only model updates are shared,

preserving user privacy while still allowing the development of powerful, data-driven systems. In the SSI context, federated learning allows credential issuers, verifiers, and service providers to collaborate on improving fraud detection, authentication, or risk assessment models without compromising the confidentiality of personal data.

Complementing this, confidential computing leverages secure hardware enclaves to process sensitive data in isolated environments, ensuring that information remains protected even while in use. For identity systems, this means that verifiable credentials and cryptographic proofs can be processed securely without exposing underlying data to third parties. Together, federated learning and confidential computing strengthen the alignment of AI with SSI principles by combining scalability and performance with strong guarantees of privacy, integrity, and trustworthiness.

3.2.4 Autonomous AI Agents vs Generative AI

To understand how Self-Sovereign Identity (SSI) and Artificial Intelligence (AI) work together, we first need to clearly separate Generative AI (GenAI) from Autonomous AI Agents. They are very different when it comes to identity and trust. Generative AI (GenAI) creates content such as text, images, or code, based on large datasets. Examples include ChatGPT, Claude, Grok, image generators, or synthetic data tools. GenAI responds to prompts but doesn't act independently beyond specific instructions. In contrast, Autonomous AI Agents can independently interact with other parties, make decisions, and perform tasks without constant human oversight. They proactively manage tasks, make decisions, delegate work, and adapt to changes. Examples include autonomous maritime inspection systems, drone operations for inspections, or AI agents used in ERP and finance transactions.

Unique Identity and Trust Challenges

Autonomous agents face specific challenges around identity, trust, and accountability:

- **Non-Human Identities (NHIs)**: Autonomous agents need their own digital identities, clearly indicating their role, ownership, permissions, and authorized actions. Unlike human identities, these identities must explicitly show their authorization and delegation.
- **Delegation Chains:** These agents often act on behalf of people or organizations and sometimes even delegate tasks to other agents. It can be complicated to ensure that these delegation paths are valid, trustworthy, and revocable.
- **Dynamic Trust Management:** Agents operate in environments that can change quickly. They must manage permissions and

authorizations in real-time, which traditional centralized verification methods can't handle efficiently.

- **Auditability and Accountability:** Autonomous agents' actions must be traceable and auditable, ensuring accountability for all outcomes. Clear, reliable audit trails and verifiable credentials are critical.

SSI helps solve these problems using Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and cryptographic keys and proofs. SSI provides the trust-layer for verifiable identities, controlled permissions, and effective governance directly within interactions between agents and humans, making autonomous agent systems secure, verifiable, accountable, and scalable.

3.3. Relevant European Regulations

As the convergence of SSI, AI, and blockchain technology progresses, regulatory alignment becomes a critical enabler of trustworthy, scalable, and rights-respecting systems. The EU has emerged as a global leader in digital regulation, introducing pioneering legal frameworks that directly shape how digital identity and AI are developed and deployed. Three key instruments stand out: the General Data Protection Regulation (GDPR), the eIDAS 2.0 Regulation, and the AI Act. Together, they form a foundational regulatory architecture for the ethical and lawful deployment of identity and intelligence systems in Europe and beyond.

The GDPR, which came into effect in 2018, sets a global benchmark for data protection and privacy. It defines personal data as any information related to an identified or identifiable person and introduces a series of obligations for data controllers and processors, including lawful basis for processing, transparency, purpose limitation, and data minimization.

SSI frameworks are inherently aligned with these principles. Because verifiable credentials (VCs) and decentralized identifiers (DIDs) support user-centric control and selective disclosure, they enable data processing that is purpose-bound and privacy-preserving by design. Unlike traditional identity systems, where large volumes of personal data are stored by central authorities, SSI architectures avoid unnecessary aggregation and support data minimization at the protocol level, thereby reducing regulatory risk under GDPR.

Moreover, SSI's emphasis on explicit consent, revocable credentials, and cryptographic verifiability strengthens compliance with GDPR requirements for transparency and accountability. It empowers individuals to act as the stewards of their personal data, exercising rights such as access, rectification, portability, and erasure with greater ease and autonomy.

The eIDAS 2.0 Regulation, adopted in 2024 (Regulation (EU) 2024/1183), builds on the original 2014 eIDAS framework by establishing a legal basis for the European Digital Identity Wallet (EUDI Wallet). This new framework aims to provide all EU citizens and businesses with the ability to identify and authenticate themselves online across borders using verifiable credentials issued by trusted service providers. While eIDAS 2.0 does not enforce a purely SSI-based architecture, it introduces qualified digital wallets, trust frameworks, and cross-border interoperability requirements that intersect significantly with SSI technologies.

Under eIDAS 2.0, digital credentials such as diplomas, driving licenses, or professional certificates can be presented and verified using mechanisms compatible with DIDs and VCs. However, governance of these systems remains semi-permissioned, with member states and Qualified Trust Service Providers (QTSPs) playing a central role in credential issuance and validation. This raises important questions about how SSI's open and permissionless models will interface with regulated digital identity ecosystems.

Despite these structural differences, the convergence between eIDAS 2.0 and SSI offers a practical pathway for mainstream adoption of decentralized identity principles within a rights-based and legally enforceable framework. Bridging this regulatory-technical interface will be critical for achieving cross-border identity portability, while preserving individual control and systemic trust.

Another relevant regulation is the Artificial Intelligence Act (EU Regulation 2024/1689), which represents the first comprehensive legal framework for AI governance globally. It introduces a risk-based classification system, distinguishing between prohibited, high-risk, and low-risk AI applications, and mandates specific obligations for transparency, accountability, and human oversight in AI development and deployment. Similar efforts have been made in different jurisdictions.

From an identity perspective, AI systems used for biometric identification, credit scoring, eligibility assessments, and automated decision-making are classified as high-risk. Such systems must comply with strict requirements, including high-quality training data, robustness, cybersecurity, auditability, and explainability. This has direct implications for blockchain-native AI solutions that rely on identity inputs for risk scoring, fraud detection, or access control.

SSI enhances the compliance readiness of AI systems under the AI Act by providing verifiable, provenance-rich, and user-consented data inputs. This reduces the dependency on inferred or scraped data, often non-compliant with GDPR, and instead supports transparent, auditable, and trustworthy AI interactions. In turn, AI applications built on SSI-aligned inputs can better meet legal obligations related to fairness, data governance, and explainability.

Additionally, the AI Act promotes the use of regulatory sandboxes and encourages standardization efforts through collaboration with international bodies. This opens an important avenue for SSI-AI ecosystems to be tested, refined, and evaluated in a controlled yet innovative regulatory environment. Other supporting frameworks and guidelines relevant to the convergence of SSI and AI include several recent legislative instruments that reinforce digital trust, platform accountability, and user empowerment within the broader European regulatory landscape.

The Digital Services Act (DSA) introduces a new rulebook for online intermediaries and platforms, mandating greater transparency in algorithmic curation, moderation practices, and the profiling of users. For identity systems powered by AI, this means disclosing how identity-based inferences affect access, content prioritization, or eligibility. The DSA establishes obligations for platforms to provide meaningful user recourse and to conduct risk assessments for systemic impacts, which directly complements the goals of SSI in enabling user-controlled, verifiable identity flows without opaque processing or silent profiling.

The Digital Markets Act (DMA) targets large online gatekeepers that exert disproportionate control over digital ecosystems. By enforcing interoperability, data portability, and constraints on anti-competitive behavior, the DMA supports a more pluralistic identity environment in which SSI systems can coexist and interoperate with incumbent identity platforms. This creates room for decentralized identity solutions to offer alternatives to platform-centric login systems, challenging the dominance of proprietary federated identity providers and enhancing user choice.

The Cyber Resilience Act (CRA) introduces horizontal cybersecurity requirements for digital products with embedded software, including AI components. It mandates secure-by-design and secure-by-default principles, particularly around data handling, software updates, and supply chain integrity. In SSI-AI systems, where credentials may be processed or verified at the edge (e.g., in wallets, devices, or IoT endpoints), compliance with CRA helps ensure that the infrastructure managing personal identity data is resilient against compromise or misuse.

The Data Governance Act (DGA) and Data Act establish the legal framework for trustworthy data sharing in the EU, emphasizing interoperability, individual agency, and fair access. The DGA introduces mechanisms for data altruism, data intermediaries, and public-private data sharing under precise consent mechanisms. The Data Act, on the other hand, clarifies rights around co-generated data and promotes portability and access to data from connected devices. Together, these regulations support SSI's decentralization paradigm by embedding data sovereignty and purpose-bound usage into law. They enable the

creation of data ecosystems where verifiable credentials and decentralized identifiers can function seamlessly across sectors without central data monopolies.

These complementary legal instruments not only strengthen the operational and ethical foundations of SSI-AI systems but also reflect a broader normative shift toward user-centric, transparent, and interoperable digital infrastructures in Europe. For innovators and policymakers, engaging with these regulations is essential to ensuring that emerging identity and AI architectures are not only technically robust but also legally compliant and socially and ethically aligned.

4. State of the Art

4.1. SSI Projects in European and International Environments

Digital identity has evolved beyond a technical layer to become a pillar of sovereignty, competitiveness, and fundamental rights. In the new paradigm of digital trust, no country or region can claim exclusive authorship, because the architecture that sustains it — Self-Sovereign Identity (SSI) — was born from open, global standards defined by the World Wide Web Consortium (W3C). Europe, the Americas, Asia, and Africa are all building upon that shared foundation, adapting the same principles to their respective political and cultural contexts.

Europe and eIDAS 2.0: institutionalizing open standards

In a global context, Europe has been one of the regions that has most coherently adopted and institutionalized these global principles, not only translating abstract frameworks into practice but also embedding them within a structured governance ecosystem. The European Blockchain Services Infrastructure (EBSI) and the ESSIF-Lab program were both built on W3C standards, and they extend them through an additional layer of public governance, regulatory oversight, and alignment with EU data protection and cybersecurity policies. This ensures that technological innovation remains closely linked to democratic accountability and citizens' rights. Their shared goal is to allow European citizens, institutions, and businesses to issue, verify, and manage digital credentials across borders under ethical, legal, and privacy-compliant conditions, fostering trust and transparency in cross-border interactions. The programs also aim to stimulate an interoperable market for trustworthy digital services by supporting open-source tools and pilot deployments across multiple sectors, including education, healthcare, and finance.

The eIDAS 2.0 Regulation (2024/1183) formalizes this adoption at the European level, establishing the European Digital Identity Wallet (EUDI Wallet) as the

unifying application and setting standards for interoperability among Member States. Although eIDAS 2.0 operates within a partially permissioned model — with Member States and Qualified Trust Service Providers (QTSPs) acting as guarantors — its technological foundation remains fully compliant with SSI standards, as defined by the W3C. Core components such as Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and interoperable trust frameworks mirror those implemented in other regions, including Latin America, Asia, and Africa. In this regard, Europe does not lead through invention but through its capacity to regulate, institutionalize, and scale digital identity frameworks responsibly, positioning itself as a global reference point for governance-driven digital innovation.

Global Case Studies: Interoperability in action

Initiatives such as QuarkID in Buenos Aires, MOSIP across Asia and Africa, and Identus on the Cardano network demonstrate that W3C standards are independent of any single region or jurisdiction. This illustrates that decentralized identity principles can adapt to highly diverse political, technological, and cultural contexts. These implementations highlight a growing global consensus on the need for open, interoperable, and privacy-preserving identity solutions that reduce dependence on centralized authorities. In all cases, the technical foundation is identical and relies on a combination of key components designed to ensure trust, transparency, and user control over data:

- **Decentralized Identifiers (DIDs)** serve as cryptographically verifiable digital identifiers that enable individuals and organizations to establish secure, persistent, and self-managed identities without reliance on a central authority.
- **Verifiable Credentials (VCs)** provide a standardized method for issuing, presenting, and verifying digital attestations such as diplomas, licenses, or government documents, ensuring data integrity and authenticity across different systems and jurisdictions.
- **Governance models** define the institutional, legal, and procedural frameworks that balance sovereignty, privacy, and regulatory compliance. They determine who can issue and verify credentials, establish trust between participants, and manage disputes or revocations.

Strategic Lessons

From this worldwide convergence, several structural insights emerge:

- Interoperability is not geopolitical — it is semantic. The ledger may differ, but the meaning of a credential must remain universal. Real interoperability depends on standards, not jurisdictions.

- Trust cannot be imposed — it must be negotiated. Each ecosystem blends regulation, ethics, and technology differently. The global challenge is to make those variations bridgeable rather than exclusionary.
- Europe regulates, W3C defines. Europe's strength lies in translating global technical standards into public policy, while SSI's legitimacy stems from its community-driven, decentralized origins.

4.2. Blockchain Platforms and Protocols for Decentralized Identity

The Linux Foundation Decentralized Trust (LFDT) hosts a number of open-source projects for decentralized identity. Among its key identity-focused projects, Hyperledger Indy is a distributed ledger that provides tools, libraries, and reusable components for creating and using independent digital identities. Hyperledger Identus provides components to develop decentralized identity solutions that adhere to widely recognized self-sovereign identity (SSI) standards. It offers complete DID and verifiable credential functionality and simplifies the complexities of adopting a decentralized identity solution into existing and new workflows. The Hyperledger AnonCreds specification, which operates under the Linux Foundation Community Specification License, enables privacy-preserving verifiable credentials that can be exchanged using the W3C Verifiable Credential Data Model with Data Integrity proofs.

CREDEBL, recognized as a Digital Public Good by the UN-endorsed DPG Alliance, serves as an open-source platform for national digital ID projects in Bhutan and Papua New Guinea, integrating contributions from Hyperledger Indy and Trust over IP as well as OpenWallet Foundations ACA-Py and Credo. The platform is designed to be multi-tenant, agent-agnostic, and ledger-agnostic, providing flexibility across different Verifiable Data Registries, DID methods, and Verifiable Credential formats. Complementing these technical projects, Trust over IP (ToIP) provides the governance layer, defining a complete architecture for Internet-scale digital trust that combines cryptographic trust at the machine layer with human trust at the business, legal, and social layers.

The ToIP stack consists of four layers with both technology and governance components, where governance frameworks specify the policies under which digital trust ecosystems operate. This comprehensive suite of LFDT technologies represents a mature, production-ready ecosystem for implementing decentralized identity solutions at scale, from national identity systems to enterprise applications, all built on open standards including W3C DIDs, Verifiable Credentials, and DIDComm protocols.

The future of digital identity is multilateral and modular, with no single government or corporation dominating its evolution. Instead, cooperation among initiatives such as the OpenWallet Foundation (OWF), Decentralized Identity Foundation (DIF), Trust over IP Foundation (ToIP), World Wide Web Consortium (W3C), European Blockchain Services Infrastructure (EBSI), Modular Open Source Identity Platform (MOSIP), and QuarkID will determine the scale and resilience of this emerging ecosystem. In essence, the self-sovereign identity (SSI) landscape is evolving into a shared civilizational infrastructure, grounded in open standards, distributed governance, and ethical responsibility. Europe provides regulatory leadership, Latin America contributes agility and social innovation, while Asia and Africa bring scale and inclusion. At the center, the W3C acts as a neutral framework that connects these diverse efforts, ensuring the world speaks a common language of trust, verifiability, and digital sovereignty.

4.3. Advances in AI Applied to Identity and Verification

Artificial intelligence is redefining the very notion of digital authenticity. For decades, identity verification relied on static processes such as passwords, databases, forms, and credit scores—mechanisms that all established trust through fixed credentials. Today, this paradigm is giving way to intelligent and adaptive systems that learn from behavioral patterns, contextual signals, and dynamic trust relationships to validate identity in a continuous, contextual, and secure manner.

From one-time authentication to continuous trust

AI enables the transition from one-off authentication to continuous, context-aware verification, where machine learning models identify subtle behavioral anomalies—such as keystroke rhythms, voice cadences, movement trajectories, and device usage patterns—to distinguish legitimate users from impostors with unprecedented precision. These algorithms operate without the need to store sensitive biometric data in centralized servers, thereby reducing privacy risks. When combined with Decentralized Identifiers (DIDs) and Zero-Knowledge Proofs (ZKPs), they enable identity validation without revealing personal information. In this way, AI and SSI converge to establish a probabilistic, adaptive, and decentralized model of trust, transforming identity from a static credential into a dynamic signal stream continuously verified through cryptography.

AI and decentralized biometrics

Computer vision, speech analysis, and multimodal recognition systems are converging toward decentralized biometrics, where data capture and validation occur locally through edge computing and outputs are registered as Verifiable Credentials (VCs). This architecture reduces risks of surveillance and manipulation

while enabling privacy-preserving authentication. A "verified face" or "voice credential" can be issued by a certified system but remain entirely under the user's control within their SSI wallet, allowing selective disclosure without exposing personal data. In this model, AI does not own an identity but interprets it temporarily to provide verifiable context and confidence. Each authentication becomes a cryptographically auditable event that contributes to decentralized reputation systems that learn from verified behavior rather than bias, embedding accountability into digital trust.

The cognitive KYC revolution and verifiable reputation

Traditional KYC models rely on centralized databases that are prone to leaks, duplication, fraud, and regulatory overhead, creating both security and efficiency challenges. These systems typically reduce identity verification to a bureaucratic checklist rather than a living process, leaving institutions vulnerable to outdated or falsified data. By contrast, the cognitive KYC paradigm merges verifiable credentials, AI-driven agents, and distributed reputation systems to build a continuously validated understanding of identity. In such a model, identity is not only confirmed at a specific point in time; it is continually contextualized and re-evaluated as users interact within financial, social, and digital ecosystems.

Rather than evaluating "who you are" solely through static credit scores or limited financial histories, AI analyses verifiable behaviors, peer attestations, transaction patterns, and cross-domain trust interactions to develop an evidence-based identity profile. This transforms the notion of identity into a living trust profile, one that evolves and strengthens through verified participation and transparent interactions rather than opaque institutional scoring. These new forms of verification are already being piloted in decentralized finance (DeFi), digital health, and e-governance ecosystems, where verifiable data and AI-driven analytics enhance both security and inclusiveness.

In each of these contexts, AI functions as a guardian of system integrity, ensuring coherence, detecting anomalies, and enabling adaptive compliance — but always within the boundaries of user sovereignty and informed consent. The result is a new generation of trust engines that combine intelligence, cryptography, and accountability, redefining how digital reputation, compliance, and ethical governance can coexist. Embedding transparency and decentralization into the KYC process offers a path toward a more trustworthy and equitable digital infrastructure that handles identity as an evolving relationship between individuals, institutions, and intelligent systems.

Synthetic identities and autonomous AI agents

The rise of autonomous AI agents also adds a new layer of complexity to digital trust and governance. As artificial intelligences act independently on behalf of

individuals or organizations, verifying and authorizing their actions becomes essential. VCs and DIDs link each cognitive agent, for example, conversational assistants and financial bots, to a verifiable identity, ensuring accountability and transparent boundaries for decision-making. Rather than serving as static proofs, verifiable credentials evolve with the agent's behavior, encoding permissions, ethical constraints, and reputation indicators. This enables machine-to-machine transactions with integrity comparable to human systems while reducing impersonation risks and being governed by SSI principles. Soon, cognitive agents—from digital assistants to autonomous vehicles—will hold their own DIDs and cryptographic trust anchors. These tools will let them authenticate, negotiate, and collaborate securely without intermediaries, establishing a decentralized layer of algorithmic trust where humans and machines operate with equal transactional legitimacy.

From electronic passports to living trust ecosystems

AI does not replace identity—it amplifies and contextualizes it within a broader socio-technical fabric of trust. Verification becomes an ongoing and adaptive process, where every action, transaction, and interaction either strengthens or weakens an entity's trust score based on verifiable behavior and cryptographic evidence. In this new landscape, digital identity is no longer a passport or a database entry; it becomes a dynamic ecosystem of verifiable trust, dynamically adapting to context, consent, and interaction history.

The convergence of AI and SSI establishes the foundation for a new global trust architecture—one that embeds accountability and interpretability at its core. Together, AI and SSI enable systems capable of learning, adapting, and self-correcting based on verifiable evidence rather than probabilistic inference. The outcome is a model of cognitive, auditable, and human-centered trust in which algorithms do not replace the subject but instead empower individuals to be recognized with truth, context, and digital dignity, ensuring that fairness and autonomy are encoded directly into the system architecture.

4.4 Advances in Trusting AI

The global race to develop increasingly capable AI systems has exposed a structural paradox: the smarter the algorithm, the harder it becomes to trust. In response, a new discipline is emerging — Trustworthy AI — and its convergence with Self-Sovereign Identity (SSI) is giving rise to the first auditable intelligence ecosystem in human history.

From blind automation to verifiable intelligence

Traditional AI often operates as a black box—models generate predictions, yet the provenance of data, the rationale behind decisions, and the accountability chain

frequently remain opaque. Embedding SSI principles directly into AI workflows transforms this paradigm by making every data point, model, and decision cryptographically anchored and traceable. In such a system, training datasets become verifiable credentials, model releases are issued as digitally signed artifacts, and each inference carries metadata detailing its provenance, accuracy, and ethical constraints. This integration shifts AI from a paradigm of automation without context to one of intelligence with lineage, where transparency and accountability are intrinsic design features.

Provenance: the memory of machines

In an SSI–enabled ecosystem, provenance ensures that every AI component — whether data, model, parameter, or output — has a unique decentralized identifier (DID) and an immutable signature of origin. This structure allows auditors and users to verify not only the source of the data but also the specific consent, license, and intended purpose under which it was gathered and used. By embedding verifiable provenance throughout the AI lifecycle, SSI technology closes the trust gap between model creators, regulators, and end users, effectively establishing a transparent chain of custody for digital knowledge. As a result, the concept of "responsible data" becomes measurable, auditable, and enforceable.

Explainability: Turning decisions into evidence

Explainable AI (XAI) has long been a research ambition, and SSI introduces the missing layer of verification. When each model and dataset is linked to a DID and verifiable metadata, explanations cease to be rhetorical narratives and instead become cryptographic attestations. This means that an AI decision can point to the specific credentials that informed it, the contextual conditions under which it was made, and the governance rules that constrained it at that moment. Such transparency elevates explainability from a desirable feature to a compliance-grade mechanism of accountability, aligning AI behavior with ethical, legal, and societal norms.

Governance: Decentralized oversight and algorithmic accountability

Trustworthy AI requires governance mechanisms that match its scale, complexity, and autonomy. Rather than relying on centralized authorities to certify opaque, black-box systems, decentralized governance frameworks — built on blockchain and SSI — enable distributed oversight. Through smart contracts, lifecycle policies can be automatically enforced, model credentials revoked, and audits triggered when anomalies arise. Cross-institutional trust registries further strengthen accountability by recording which models are certified, deprecated, or under review, ensuring global traceability without introducing a single point of control. In this paradigm, governance turns into programmable trust—a dynamic,

verifiable layer of assurance that aligns AI systems with ethical and regulatory expectations.

Ethical alignment through verifiable consent

AI systems increasingly interact with human data, creativity, and emotion, blurring the boundaries between technological autonomy and human agency. SSI brings consent back to the center of this relationship: individuals can issue, restrict, or revoke credentials that determine how their data or likeness is used to train or interact with AI. This framework establishes the foundation for human-centric alignment, ensuring that the autonomy of AI systems remains balanced by the digital rights and intentions of their contributors. Each dataset, avatar, or synthetic twin involved in AI training can thus be linked to a verifiable record of consent, providing an enforceable mechanism for data ethics at scale.

Toward a transparent cognitive economy

When AI becomes verifiable and identities are self-sovereign, the transparent cognitive economy emerges. In such an ecosystem, data, models, and insights circulate as authenticated digital assets, each carrying cryptographic proof of origin, licensing terms, and integrity. Enterprises can exchange verified AI services, regulators can audit models in real time, and citizens can interact with algorithms that are accountable by design. In this context, trust is no longer an abstract matter of belief—it evolves into a computable property.

The new social contract of intelligence

Trust in AI is not granted by default — it is constructed through verification processes. The convergence of SSI and AI redefines the social contract between humans and machines, ensuring that every intelligent action is attributable, auditable, and explainable. Provenance establishes what occurred, explainability clarifies why it happened, and governance delineates who holds responsibility. Together, these three pillars form the basis for an AI ecosystem where intelligence becomes a public good: transparent, ethical, and interoperable across institutional and national boundaries.

4.5 Identity and Trust for Autonomous AI Agents

Autonomous AI agents have unique identity and trust challenges because they operate independently, make decisions on their own, and can directly impact real-world situations. Self-Sovereign Identity (SSI) can use Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and Trust Registries to handle these challenges effectively.

- **Decentralized Identifiers (DIDs):** DIDs give each autonomous agent a unique digital identity without depending on any central authority.

Anchored in decentralized systems such as blockchains, DIDs allow agents to identify themselves and verify others independently securely. This decentralized verification is essential when multiple agents from different organizations interact regularly.

- **Verifiable Credentials (VCs):** VCs clearly show an agent's roles, permissions, and authorizations. Trusted entities such as governments, companies, or regulatory bodies issue these digital credentials. VCs make it explicit what an agent can do and under what conditions. For example, maritime inspection agents hold credentials proving their authority to inspect cargo or enforce environmental regulations. VCs eliminate confusion, making agent interactions clearer and safer.
- Tr**ust Registries:** Trust registries are decentralized directories listing trusted entities, their credentials, and allowed actions. They help agents quickly confirm that other agents and stakeholders have valid, current credentials. For instance, trust registries ensure drone operations can quickly verify operator credentials, significantly streamlining processes and enhancing trust.
- **Interoperability:** Minimal interoperability standards, such as the "Web of Agents" framework, enhance communication and cooperation across agent systems. These standards reduce complexity and help avoid fragmented ecosystems, making it simpler and more secure for agents to interact seamlessly across different platforms and environments.

4.5.1 Delegation and Credential Revocation in Multi-Agent Environments

Delegation and revocation are critical in multi-agent environments, where multiple autonomous AI agents interact, cooperate, or even compete, and require sophisticated management and control approaches:

- **Delegation Management**: In multi-agent systems, delegation happens frequently and can form complex chains. Agents can act on behalf of humans or other agents, passing responsibilities down multiple layers. SSI can address this complexity by providing detailed, cryptographic records that clearly trace each step of the delegation path. These delegation chains explicitly document who granted permissions, to whom, and under what specific conditions. This detailed visibility helps quickly detect and prevent unauthorized delegations or misuse of delegated authority.__In parallel, organizations need to define clear role boundaries, permitted actions, and escalation procedures to human decision-makers,

ensuring that technical delegation controls are supported by governance policies.

- **Credential Revocation:** Rapid and reliable credential revocation is essential to maintaining trust in multi-agent ecosystems. SSI supports advanced revocation methods such as status registries or revocation lists, ensuring immediate updates across the decentralized network. This fast revocation capability is crucial when responding to security breaches, changes in roles, expired permissions, or policy updates. They act like a “kill-switch” and guarantee that revoked credentials no longer grant access or permissions immediately after revocation, preventing potential misuse or security incidents.
- **Real-Time Verification:** Multi-agent systems often require real-time or near-real-time verification of credentials and delegations. SSI's decentralized infrastructure ensures continuous availability and high responsiveness, supporting quick verification even in highly dynamic environments. This capability is particularly valuable for critical operations, such as autonomous vehicle management, real-time financial transactions, or regulatory compliance inspections.
- **Audit Trails:** SSI inherently supports robust audit trails through decentralized logging of credential usage, delegation actions, and verification requests. These audit trails provide transparent and immutable evidence of agent actions, enabling thorough reviews and compliance audits. Auditability significantly enhances accountability and trustworthiness, especially in regulated industries or high-risk scenarios.

By integrating DIDs, VCs, trust registries, and advanced delegation and revocation capabilities, SSI technologies provide a comprehensive, reliable foundation for identity and trust management in autonomous AI agent environments, supporting secure, verifiable, accountable, and efficient operations.

4.5.2 Governance and Accountability

Governance and accountability are critical when autonomous AI agents operate independently. These agents must be clearly accountable for their decisions and actions, especially when impacting real-world situations.

Maintaining Accountability

To ensure accountability, every agent's action must be clearly traceable back to the responsible parties. This involves assigning explicit ownership, clearly defining authority, and creating reliable ways to monitor and verify actions. Using SSI technologies such as OpenID Federation and verifiable credentials ensures each action can be confidently traced to authorized agents.

Monitoring and Enforcement
Monitoring involves real-time tracking of agent activities to detect unauthorized or unexpected behavior quickly. Trust registries provide continuous monitoring capabilities, enabling immediate enforcement actions. Clear enforcement policies embedded directly into the SSI infrastructure allow rapid responses to policy violations or security incidents.

Auditable and Verifiable Interactions
Robust and immutable audit trails are essential for trust and regulatory compliance. SSI solutions ensure every interaction and decision-making step is transparently documented. This enables easy verification by stakeholders, auditors, or regulators, significantly enhancing trust and accountability.

Interoperability to Enhance Governance
Minimal interoperability standards help avoid fragmented ecosystems, improving security, openness, and scalability. For example, the "Web Of Agents" framework identifies four critical building blocks:

- Agent-to-Agent Messaging: Simplifies secure communication between agents.
- Interaction Interoperability: Makes sure agents clearly understand each other's requirements and interfaces.
- State Management: Provides reliable short-term and long-term state tracking.
- Agent Discovery: Enables agents to find and collaborate with suitable partners efficiently.

This approach prevents isolated, incompatible agent systems, reduces complexity, and strengthens the overall trust and governance of autonomous AI ecosystems. Overall, integrating SSI ensures effective governance, clear accountability, and reliable auditability, which are critical for the successful operation of autonomous AI agent ecosystems.

5. Synergies between SSI and AI

The convergence of Self-Sovereign Identity (SSI) and AI represents a paradigm shift in how digital trust is operationalized. SSI provides cryptographically verifiable, user-controlled identity artifacts, while AI transforms these into actionable intelligence for fraud prevention, decision-making, and automation. The synergy lies in the complementarity: SSI guarantees the provenance and integrity of data, and AI enhances its usability, efficiency, and scale.

5.1. The Role of AI in Credential Verification and Fraud Detection

AI models can efficiently validate verifiable credentials by detecting inconsistencies, anomalies, or tampered proofs across large datasets in real time. Machine learning algorithms enhance fraud detection by identifying patterns invisible to traditional rule-based systems, such as behavioral anomalies or synthetic identity fraud. When combined with SSI, AI ensures that credential verification is both cryptographically secure and dynamically adaptive.

5.2. Optimizing User Experience (UX) and Process Automation

AI-driven orchestration reduces friction in SSI workflows. For example, AI agents can auto-fill forms, suggest minimal disclosure proofs, or streamline onboarding by predicting which credentials are required for a given service. This reduces cognitive load for users and operational costs for providers. Natural Language Processing (NLP) and conversational AI further humanize SSI interactions, making digital identity processes intuitive and accessible.

5.3. Explainable AI (XAI) and Transparency in Identity Decision-Making

Integrating XAI with SSI ensures that every identity-related decision can be justified, audited, and explained. When an SSI credential is rejected, XAI frameworks can clarify whether the cause was cryptographic invalidity, policy mismatch, or risk scoring anomalies. This transparency is critical for maintaining institutional trust and regulatory compliance in high-stakes contexts such as finance, healthcare, or e-government.

5.4. Application Scenarios

- **DeFi:** SSI–backed KYC credentials, when combined with AI-driven fraud detection, enable lightweight yet compliant onboarding processes. This approach enhances privacy and reduces exposure to identity theft.
- **Government Services:** AI and SSI together enhance public administration by automating eligibility verification for welfare, taxation, or voting systems. This integration promotes fairness, reduces bureaucratic overhead, and enhances citizen trust in digital governance through verifiable credentials and transparent decision processes.

- **IoT:** SSI provides a secure and verifiable identity layer for connected devices, while AI continuously monitors behavioral patterns to detect anomalies. This combination safeguards human–machine and machine–machine interactions, ensuring the resilience and integrity of critical infrastructures.

5.5 AI as the Multi-Blockchain and Protocols Compatibility Agent

One of the main challenges in SSI adoption is cross-protocol interoperability. AI can act as a dynamic compatibility agent across heterogeneous ecosystems by mapping schemas, resolving DID methods, and ensuring seamless interaction across multiple blockchains and identity frameworks. This "AI interoperability layer" enables SSI to operate fluidly across financial institutions, government infrastructures, and decentralized networks.

5.6. SSI and Proof of Humanity in Multi-Agent AI Ecosystems

As the AI industry evolves toward multi-agent systems—comprising autonomous agents, orchestrators, and self-adaptive ecosystems—the boundaries between human and machine actors will blur. In such environments, trust depends not only on verifying the authenticity of credentials but also on distinguishing whether the counterpart is a human or an AI entity. SSI must therefore extend beyond traditional identity functions to enable Proof of Humanity (PoH) and related mechanisms that ensure authenticity in online interactions.

Future SSI frameworks are expected to incorporate advanced cryptographic attestations capable of proving human uniqueness and preventing Sybil attacks, while simultaneously supporting machine identities for autonomous AI agents. This dual structure will make it possible to manage hybrid ecosystems where humans and AI agents collaborate seamlessly but remain distinguishable. By embedding PoH into verifiable credentials, SSI ensures that critical operations such as voting, financial transactions, medical consultations, and governance decisions remain safeguarded against the risks of impersonation or synthetic identity manipulation.

In this sense, SSI not only serves as the trust fabric for human identity but also becomes the gatekeeper of authenticity in a world where AI systems act autonomously and at scale. This new dimension—verifiable proofs of humanity—will be foundational to guaranteeing fairness, accountability, and resilience in the AI-driven digital economy.

6. Design and Architecture of Combined Solutions

The successful convergence of Self-Sovereign Identity (SSI) and Artificial Intelligence (AI) requires more than isolated technological components; it demands a cohesive architecture that integrates verifiable identity, decentralized infrastructure, and privacy-preserving intelligence. This architecture must balance scalability, security, transparency, and compliance across different jurisdictions and industries, while remaining flexible enough to adapt to new governance and regulatory frameworks. A combined SSI–AI design paradigm introduces three core requirements:

- Trust by design – leveraging verifiable credentials, decentralized identifiers, and immutable registries to ensure the provenance of identity inputs.
- Privacy by design – embedding advanced cryptography, differential privacy, and federated learning to minimize personal data exposure while maximizing utility.
- Scalability by design – ensuring interoperability across blockchains, institutions, and AI ecosystems through open standards and modular architectures.

These principles enable a future-proof ecosystem where human and AI agents can interact securely, verifiably, and ethically, supporting high-value use cases such as finance, healthcare, e-government, and autonomous systems.

6.1. Integrating SSI into Blockchain/DLT Infrastructures

Blockchain and Distributed Ledger Technologies (DLTs) provide the foundational trust layer for SSI by anchoring decentralized identifiers (DIDs), credential revocation registries, and trust registries. The integration of SSI into DLT infrastructures follows a layered architectural model:

- Identity Layer: DIDs and Verifiable Credentials are issued, stored in user-controlled wallets, and presented to verifiers through selective disclosure.
- Blockchain Trust Layer: Distributed ledgers anchor DID documents, revocation lists, and governance rules, ensuring immutability and auditability without requiring constant connection to issuers.
- Service and Application Layer: AI modules consume SSI-verified data, applying fraud detection, risk scoring, or eligibility checks based on verifiable proofs rather than opaque data brokers.

Integration challenges include:

- Latency: Blockchain validation may introduce delays in real-time AI-driven decisions (e.g., instant payments, IoT device authorization).
- Cost Efficiency: Transaction fees and gas costs may hinder scalability for high-volume SSI use cases.
- Governance Alignment: National and sectoral governance frameworks (e.g., eIDAS 2.0 in the EU, NIST standards in the U.S.) must align with open SSI standards to ensure cross-border interoperability.

Emerging solutions include layer-2 scaling approaches, off-chain credential verification with on-chain proofs, and hybrid infrastructures where blockchain is used selectively for auditability and trust anchoring. These patterns ensure that SSI can be both globally interoperable and locally compliant, addressing the dual imperatives of scalability and regulation.

6.2. Distributed AI Processing Models and Differential Privacy

Integrating AI into SSI ecosystems requires architectures that can process sensitive identity data without compromising privacy. Traditional centralized AI pipelines are not suitable for SSI, as they reintroduce risks of data concentration and surveillance. Instead, distributed AI models align naturally with SSI principles:

- Federated Learning: Models are trained locally on user or institutional devices using SSI-verified data. Only model updates, not raw data, are shared with aggregators. This ensures that sensitive information (biometric proofs, financial history, health credentials) remains decentralized.
- Confidential Computing: Trusted Execution Environments (TEEs) and Confidential Virtual Machines (CVMs) provide secure enclaves where identity-sensitive AI processes can occur without exposing raw inputs to operators or third parties.
- Differential Privacy: By injecting controlled statistical noise, differential privacy ensures that aggregated insights cannot be reverse-engineered to expose individual identities. This is particularly relevant in regulated domains such as healthcare and finance, where even anonymized datasets can risk re-identification.

Together, these mechanisms enable AI-driven decision-making that is both high-performing and compliant with privacy regulations such as GDPR and the EU AI Act. More importantly, they allow SSI to serve as the trust anchor for AI

training data, ensuring that models are built on provenance-rich, user-consented, and verifiable inputs rather than opaque datasets.

This distributed paradigm also supports cross-sector collaboration. For example, healthcare institutions across different jurisdictions can train predictive models using SSI-verified patient credentials, while preserving patient privacy and ensuring auditability of both the training process and the model outputs.

6.3. Standards and Interoperability

Interoperability is the lifeblood of the SSI–AI ecosystem; without it, decentralization risks fragmenting into an archipelago of technological islands. Europe—and the world—requires a common language that enables credentials, agents, and intelligences to communicate seamlessly across blockchain infrastructures and jurisdictional boundaries. At the technical level, the building blocks for this interoperability already exist.

The W3C Decentralized Identifiers (DID) and Verifiable Credentials (VC) standards ensure that digital identities can be recognized universally without reliance on a central custodian, while DIDComm v2 introduces a secure peer-to-peer messaging layer through which both humans and autonomous agents can exchange credentials and establish real-time trust. Complementing these innovations, OpenID for Verifiable Credentials bridges the legacy Web2 environment with the emerging Web3, integrating decentralized authentication into existing infrastructures.

At the semantic level, frameworks such as Data Mesh and Data Fabric enable identity-related data to travel across domains without losing context, allowing sectors such as health, education, and finance to maintain their sovereignty while connecting through shared semantic contracts. Within this architecture, artificial intelligence serves as a universal translator, mapping, interpreting, and harmonizing meanings among previously disconnected ecosystems. At the governance level, initiatives such as Trust over IP (ToIP), the OpenWallet Foundation (OWF), and the European Blockchain Services Infrastructure (EBSI) establish clear principles for interoperability, verification, and auditability. Meanwhile, Europe is also anticipating the future through post-quantum cryptography (NIST PQC), which ensures the long-term resilience and security of its systems.

Specifically, Europe and global bodies are preparing for post-quantum standards by adopting NIST PQC algorithms (ML-KEM, ML-DSA, SLH-DSA) that ensure the cryptographic longevity of their systems. Collectively, these standards and frameworks constitute the grammar of a new Internet of Trust, which is an infrastructure where SSI and AI do not compete for control over data but collaborate to preserve its meaning, integrity, and legitimacy.

6.4. Implementation Patterns and Scalability Challenges

The deployment of the SSI–AI ecosystem at an industrial scale is not merely an engineering challenge; it is a choreography of distributed trust, where every component — identity, blockchain, intelligence, and governance — must act in perfect synchronization. The implementation patterns now emerging across Europe and other regions operate as living laboratories, where emerging technologies, decentralized governance models, and new approaches to semantic and technical interoperability converge.

Hybrid Models and Composable Architectures

Among the most consolidated patterns in decentralized identity are hybrid anchoring models, in which personal data remains off-chain while only the elements required for verification, such as hashes, revocation registries, trust policies, and consent metadata, are recorded on the blockchain. This architectural approach reflects a growing recognition that verifiability and privacy are not opposing forces but complementary dimensions of trust.

By decoupling sensitive information from public ledgers, hybrid anchoring enhances both security and regulatory compliance, ensuring alignment with frameworks such as GDPR and other emerging global privacy standards. This approach, adopted by initiatives such as EBSI, QuarkID, and Identus, strikes a balance between transparency and accountability, while maintaining confidentiality. It reduces operational costs, optimizes verification latency, and supports scalability without compromising integrity. Many of these systems also employ selective disclosure mechanisms and zero-knowledge proofs to minimize data exposure while maintaining verifiable authenticity.

Complementing these advances are composable architectures that enable interoperable modules—identity, credentials, messaging, payments, reputation, and audit—to interact under the principle of decentralized plug-and-play. These architectures enable the assembly of complex identity solutions from standardized building blocks, thereby accelerating innovation, reducing vendor lock-in, and fostering cross-domain collaboration. They also create an environment in which digital identity services can integrate seamlessly with domains such as finance, health, education, and commerce. Through this model, digital identity integrates dynamically with other layers of the ecosystem, producing a flexible, adaptive, and modular fabric of trust that can evolve and adapt over time.

Agent-Oriented Architectures

A key pattern in decentralized identity systems is the rise of agent-oriented architectures, where each wallet—human, corporate, or AI-driven—acts as an

autonomous entity that manages permissions, signs transactions, verifies credentials, and executes smart contracts. In this model, artificial intelligence functions as the cognitive orchestrator of the ecosystem, anticipating interactions, reducing friction, and ensuring regulatory compliance in real time. These cognitive agents, equipped with verifiable credentials and behavioral rules, form the core of a new digital infrastructure that connects individuals, institutions, and machines through a shared language of trust. Over time, such agents will expand beyond identity management to coordinate complex interactions, such as trade, research, and data exchange, while preserving privacy and transparency. Together, they enable a dynamic, self-regulating digital environment that reflects the adaptability and resilience of human society.

Scalability: From Technical Throughput to Cognitive Scalability

Scalability remains one of the most significant challenges of decentralized AI ecosystems. SSI–AI frameworks must handle millions of verifications per second while maintaining coherence across heterogeneous blockchain environments, such as Cardano, Ethereum, Hyperledger, Solana, and Polygon, and align with evolving regulatory regimes such as eIDAS 2.0 and the EU AI Act. However, scalability extends beyond throughput. It also encompasses cognitive scalability, pertaining to the system's ability to adapt to changing contexts, dynamic policies, and human behavioral patterns.

Emerging solutions include:

- **Layer-2 rollups and optimized sidechains** which reduce network congestion and transaction costs.
- **Next-generation Zero-Knowledge Proofs (ZKPs)** allow large-scale validation without compromising privacy.
- **Interoperable multichain infrastructures**, capable of federating multiple SSI networks under W3C standards.
- **AI-assisted governance**, dynamically adjusting rules, compliance thresholds, and audit protocols in response to context, risk, and jurisdiction.
- **Edge identity verification**, enabling local validation directly on devices without continuous on-chain reliance.

Together, these approaches form the foundation of a self-scaling trust ecosystem, where security, efficiency, and adaptability expand in line with user participation and data complexity.

Cross-Chain Patterns and Shared Semantics

Cross-chain trust has emerged as a fundamental enabler of SSI–AI scalability. Standardized communication protocols, such as DIDComm v2, Hyperledger Aries,

and OpenID4VC, facilitate the seamless exchange of verifiable credentials and authenticated messages across diverse blockchain and institutional ecosystems. In parallel, Data Mesh and Data Fabric architectures provide the semantic coherence required for interoperability at scale. By preserving meaning and context as identity data moves across infrastructures, sectors, and national borders, they prevent the fragmentation of digital trust. Together, these mechanisms form the backbone of a globally interoperable trust fabric that is capable of supporting AI systems that are both decentralized and accountable.

Social Scalability and User Experience

But technological scalability is only half the equation. The true expansion of the SSI–AI model depends on human adoption, education, and cultural acceptance, as no architecture can succeed if citizens, professionals, and organizations do not understand how to use it or fail to perceive its value. Trust must be cultivated through transparency, accessibility, and meaningful user experience design that makes complex identity processes intuitive and empowering. The future of self-sovereign, AI-powered identity will therefore be measured not in transactions per second, but in trust per interaction—a new metric that reflects reliability, data stewardship, and human-centric design.

In this emerging paradigm, AI functions as the invisible interface of the digital citizen, learning from context and intent to anticipate needs and simplify experiences until proving one's identity becomes as natural as speaking or breathing. Intelligent agents will integrate seamlessly into daily life—opening accounts, accessing healthcare, signing contracts, verifying licenses, and performing countless other tasks—without technical friction or cognitive overload. These systems will adapt to individuals' preferences and regulatory environments, ensuring that every interaction remains both personalized and compliant. Ultimately, self-sovereign digital identity will evolve from a technological construct into an everyday experience of autonomy, privacy, and verifiable trust.

7. Challenges and Risks

The promise of SSI–AI does not come without shadows. Every technological revolution reshapes not only systems but also power structures —and with that, it brings new risks: technical, ethical, political, and epistemic. Recognizing them is not an admission of weakness, but the first act of architectural intelligence: turning fragility into resilience through design.

7.1. Algorithmic Biases and Fairness

Algorithmic bias remains the Achilles' heel of artificial intelligence. When models are trained on incomplete or unrepresentative data, they risk systematically

excluding entire communities, reinforcing discrimination, and distorting decision-making in critical domains such as credit scoring, healthcare, and recruitment. In this regard, SSI introduces a structural antidote to this challenge: traceability. By ensuring that every data point used by AI can be traced back to a verifiable source with cryptographic proof of origin, consent, and context, SSI enables auditability at the epistemic layer. This makes it possible not only to detect bias but also to understand how and why it emerged. Verifiable credentials transform data provenance into a civic right, empowering citizens, regulators, and developers to collaboratively diversify datasets, audit algorithmic fairness, and certify training provenance. Within this new paradigm, fairness is no longer an accidental property of code but a political decision expressed through design—a measurable commitment encoded into the very architecture of digital intelligence.

7.2. Security and Protection of Sensitive Data

Digital identity has become the crown jewel of cybercrime. As SSI-AI ecosystems expand, so too do the attack vectors that threaten them: correlation attacks, deepfake identity theft, autonomous agent impersonation, and AI-driven phishing campaigns. Yet within this convergence of SSI and AI lies the potential for a dynamic and adaptive defense mechanism. In these emerging ecosystems, AI models function as behavioral sentinels that continuously monitor and analyze wallet activity, credential exchanges, and transaction patterns to detect anomalies in real time. Using machine learning and contextual reasoning, AI can identify subtle deviations that may indicate malicious intent or compromised credentials before damage occurs.

SSI provides the cryptographic layer for this security model. Zero-Knowledge Proofs (ZKPs), confidential computing, and post-quantum encryption enable authenticity to be mathematically proven without disclosing private or personally identifiable information. This ensures privacy-preserving verification and elevates cybersecurity from a reactive posture to one that is inherently proactive and self-adaptive. Beyond human users, multi-agent authentication protocols ensure trust as autonomous systems. Agents dynamically verify each other's legitimacy, exchanging verifiable credentials and cryptographic attestations before data or value transfer. Every transaction, consent, and verification leaves behind a tamper-proof audit trail, transforming trust from a declaration into a cryptographically verifiable state.

7.3. Scalability, Adoption, and Cognitive Barriers

The greatest barriers to SSI–AI adoption are not found in hardware or cryptography, but in the collective cognitive layer comprising culture, incentives, and coordination. Mass adoption depends on building shared digital literacy

among citizens, governments, and enterprises, alongside economic models that reward verifiable and trustworthy interactions. European GovTech and FinTech pilots show that well-calibrated incentive frameworks, open standards, and UX–driven design can accelerate adoption curves, but the experience is as fluid as it is secure. The SSI–AI experience must feel intuitive, not technical, ensuring that users engage naturally with digital identity systems.

To scale meaningfully, the ecosystem must also integrate AI-mediated onboarding, where intelligent assistants help users manage credentials, detect risks, and comprehend the implications of each consent decision. Adoption is therefore not merely a matter of interface design but rather a deeper process of cognitive alignment between humans and machines, where trust becomes a learned and reinforced behavior.

7.4. Regulatory and Jurisdictional Coordination

Innovation without coordination breeds fragmentation. Europe currently leads the world in regulatory convergence—through the GDPR, eIDAS 2.0, and the AI Act—yet genuine scalability demands cross-border harmonization. Without strong international collaboration, even the most advanced policies risk being implemented unevenly across jurisdictions.

The vision ahead is a Mutual Recognition Framework (MRF) for digital credentials, allowing identities verified in one jurisdiction to be automatically recognized in another, thereby fostering trust and reducing friction in cross-border digital interactions. Such a framework would rely on interoperable technical standards, transparent governance models, and a shared vocabulary of trust that transcends national boundaries. To make this vision a reality, AI-driven legal engines could interpret and translate regulations in real time, ensuring continuous compliance across borders and sectors.

Smart contracts, operating under robust legal ontologies, would function as self-enforcing compliance agents capable of adapting to evolving regulations. They could reduce administrative overhead and provide verifiable accountability. This model would transform today's fragmented regulatory maze into a living legal network, agile enough to evolve at the same pace as innovation itself, while strengthening public trust and reinforcing digital sovereignty across Europe.

7.5. Systemic Risks and Quantum Uncertainty

Beyond regulatory and ethical dimensions, the SSI–AI ecosystem faces a more profound frontier: quantum risk. The rise of quantum computing threatens to render classical cryptography obsolete, compromising the integrity of DIDs, digital signatures, and verifiable credentials. To address this challenge, Europe and global consortia are advancing post-quantum cryptographic standards (NIST PQC) and

developing hybrid trust architectures that combine classical and quantum-resistant primitives.

However, the greater challenge extends beyond cryptography but is fundamentally epistemic: How can it be ensured that autonomous AI agents remain aligned with human-defined trust frameworks? SSI provides the governance rails, but AI will continuously test its boundaries. Sustaining trust in this evolving landscape requires AI systems capable of self-auditing, able to verify not only what they know but how they know it.

7.6. The Human Dimension

As the digital world becomes more "verifiable," societies risk trust fatigue, which is a state where endless authentication erodes confidence instead of reinforcing it. Each new credential or proof adds friction, and natural interactions turn into acts of compliance. To counter this, verification systems must remain frictionless, respectful, and inclusive, building trust through simplicity. Secure yet unobtrusive verification processes in the background will become enablers rather than obstacles.

Artificial intelligence can ease this burden by handling verification invisibly, adapting to context, and preserving human dignity and spontaneity. The true ethical test is ensuring that technology protects not just data but also the right to live without constant proof. The success of SSI–AI, therefore, depends on its power to empower without surveilling, verify without dehumanizing, and connect without controlling.

8. Strategic Recommendations

The convergence of Self-Sovereign Identity and Artificial Intelligence demands synchronized evolution across policy, governance, and technology. This roadmap provides a strategic framework for how Europe —and its global partners— can move from experimentation to full-scale implementation, shaping a verifiable and human-centric trust infrastructure by 2030.

8.1 Policy

Building a trustworthy digital society demands that legal, ethical, and technological frameworks evolve in concert. Policy becomes the arena in which sovereignty, innovation, and protection meet - defining the boundaries of freedom and responsibility in the age of decentralized intelligence.

- **Reconcile decentralization, immutability, and accountability:** Maintain personal data off-chain while anchoring verifiable proofs on-chain to preserve both privacy and integrity.

- **Ensure wallet interoperability:** Align identity and credential management with eIDAS 2.0 standards and meet the high-risk AI requirements defined by the EU AI Act.
- **Uphold GDPR principles:** Treat data minimization, revocation, and purpose limitation as non-negotiable anchors rather than optional guidelines.

Together, these principles create a coherent regulatory backbone for SSI–AI ecosystems that is capable of fostering innovation while safeguarding human dignity and digital sovereignty.

8.2 Procedures

Operational excellence is the bridge between regulatory frameworks and practical deployment. Clear, auditable processes ensure that SSI–AI systems are not only compliant with legal and ethical standards but also verifiably trustworthy in real-world operation.

- **Institutionalize verifiable routines** for credential issuance, suspension, and revocation through permissioned or consortium blockchains, ensuring traceability and accountability.
- **Adopt W3C Verifiable Credential (VC) Data Models** with selective disclosure and zero-knowledge proofs (ZKPs) to balance transparency, privacy, and compliance.
- **Develop robust contingency frameworks** to address AI model drift, consensus failures, and credential recovery, ensuring resilience and system reliability throughout lifecycles.

By embedding accountability into operational workflows, decentralized ecosystems can transform compliance into a dynamic, continuous process of trust assurance—anchoring governance in verifiability and operational integrity.

8.3 Governance

Trust without governance leads to chaos, while governance without transparency breeds control. A decentralized, polycentric governance model fosters adaptability, accountability, and resilience across interconnected ecosystems. Specifically, the following governance principles emerge:

- Adopt polycentric governance frameworks using on-chain policy contracts, quorum-based decision rules, and publicly auditable logs.
- Align governance structures with the EU AI Act, OECD AI Principles, and ISO/IEC 38507 standards to ensure regulatory coherence and interoperability.

- Guarantee traceability and accountability by linking AI outputs to verified credentials, documented model versions, and immutable audit trails.

8.4 Risk

Anticipating and mitigating systemic risks is essential to maintaining trust and ensuring the long-term continuity of digital identity infrastructures. Effective resilience requires a proactive approach that integrates technological safeguards, procedural rigor, and adaptive governance. The following measures need to be taken:

- Anticipate quantum-era challenges by implementing hybrid and post-quantum cryptographic methods to future-proof data integrity and credential security.
- Mitigate consensus manipulation risks through diverse validator committees, secondary anchoring mechanisms, and layered governance models.
- Require independent audits and formal verification for smart contracts to enhance reliability and prevent systemic vulnerabilities.
- Implement continuous fairness monitoring and adversarial testing for AI systems to guarantee transparency, robustness, and ethical accountability.

By embedding these practices into operational and governance frameworks, decentralized ecosystems can evolve into resilient trust architectures that are capable of withstanding emerging technological, regulatory, and ethical challenges.

8.5 Interoperability & Standards

Interoperability is the invisible architecture of trust, enabling diverse systems, jurisdictions, and intelligences to communicate seamlessly without friction or dependency. A robust interoperability framework ensures that digital identities, data exchanges, and AI systems operate seamlessly across technological and regulatory boundaries.

- Adopt global standards such as W3C DIDs, VCs, and DIDComm protocols to guarantee cross-platform and cross-chain compatibility across ecosystems such as Hyperledger, Ethereum, and Sovrin.
- Harmonize data and AI semantics with ISO/IEC 5259 and establish cloud interoperability frameworks to maintain consistency and data integrity.

- Prepare for post-quantum transitions by designing identity and AI infrastructures that evolve into quantum-resistant cryptographic models.

Through these principles, interoperability becomes not just a technical specification but a cornerstone of trustworthy, decentralized collaboration on a global scale.

8.6 Monitoring

Continuous assurance transforms compliance from a static requirement into a living process. Through continuous monitoring and cryptographic validation, SSI and AI systems remain transparent, auditable, and adaptive to real-world changes. The following monitoring measures need to be taken:

- Shift from static dashboards to adaptive monitoring loops, integrating third-party cryptographic audits for real-time verification and accountability.
- Leverage blockchain as a checkpoint ledger for maintaining the integrity and traceability of identity assurance and operational performance.
- Employ digital twin simulations to rigorously test SSI–AI architectures under variable and high-stress conditions before deployment.

By embedding these practices, organizations can transform assurance into a living system in which verification, accountability, and trust evolve continuously alongside technology.

9. Human-Centric Roadmap

Technology must ultimately serve people, not the other way around. Embedding human-centric principles ensures inclusion, accessibility, and ethical alignment throughout the ecosystem. Several guiding principles exist:

- Advance Equity and Access (SDGs 4, 10, 16): Digital wallets must include marginalized groups through multilingual, adaptive, and accessible interfaces. Equity must be integral to design, not an afterthought.
- Build Identity Literacy: Citizens and institutions need to understand digital identity implications and manage them safely through targeted literacy efforts.
- Engineer for Sustainability: Systems should emphasize efficiency, modularity, and maintainability along their lifecycle.

- Institutionalize Decentralized Cyber-Ethics: Governance must embed fairness, privacy, and accountability into technical systems through real-time ethical safeguards.

Together, these principles form a coherent framework for human-centric, equitable, and sustainable technology ecosystems, which ensures that innovation consistently aligns with societal values and global sustainability goals.

Humanity stands at a historic crossroads. The convergence of SSI and AI is not just a technological evolution, but a defining turning point in how civilization defines truth, agency, and collective trust in the digital era. The question before us is not whether we will use these technologies, but how we will govern them —and for whom. The coming decade will determine whether the digital world becomes a space of empowerment or domination. As nations, corporations, and algorithms compete for control over data and cognition, the world must unite behind a new principle: trust as a shared global commons. Like air, oceans, and climate, digital trust is now a planetary resource —and protecting it is a shared responsibility that transcends borders, ideologies, and markets.

The universal mission is to establish a Global Trust Infrastructure that empowers individuals, ensures algorithmic accountability, and harmonizes technological innovation with ethical governance. In this regard, blockchain offers the immutability to anchor truth; AI provides the intelligence to adapt and evolve, and SSI restores personal sovereignty while enabling cooperation at scale. This is not a race for dominance, but a collective call to stewardship in which governments, international organizations, academia, and the private sector must collaborate to ensure that technology remains a tool of liberation and not of control.

The challenge is monumental, but so is the opportunity: to design a civilization where autonomy, transparency, and accountability are not optional ideals, but systemic realities. To realize this vision, coordinated action is needed on three global fronts:

- Policy and Governance: Develop multilateral frameworks for interoperability and digital rights recognition. Integrate SSI and AI principles into international law, data protection, and sustainable development agendas.
- Technology and Standards: Advance open protocols and verifiable AI standards that protect privacy, ensure auditability and security, and promote post-quantum resilience, all of which need to be treated as global public goods.

- Education and Social Inclusion: Foster digital trust literacy across societies so that individuals and institutions understand not only how to use technology, but how to trust and govern it responsibly.

By 2030, humanity must establish a planetary network of verifiable trust, where every human, institution, and intelligent system interacts through integrity, transparency, and respect. In this envisioned world, verification replaces surveillance, consent replaces extraction, and collaboration replaces competition. This transformation is more than a technological ambition; it represents a civilizational realignment guided by ethical purpose.

The convergence of SSI and AI will reshape how societies authenticate truth, distribute power, and safeguard freedom. Together, they offer an unprecedented opportunity to design a governance fabric co-created by the global community, rather than imposed by any single entity or nation.

The Promise of a Trusted FutureTrust will evolve from being an assumption to becoming a shared global achievement. Sovereignty will depend not on borders but on cryptographic integrity, and intelligence will cease to threaten humanity — instead, it will help us rediscover what it truly means to be human.

10. References

Akin, D., & Kale, M. (2023). *Zero Knowledge Proofs: A Comprehensive Review of Applications, Protocols and Future Directions in Cybersecurity*. ResearchGate. https://www.researchgate.net/publication/373097436_Zero_Knowledge_Proofs_A_Comprehensive_Review_of_Applications_Protocols_and_Future_Directions_in_Cybersecurity

Apple Inc. (2018). *App Store Turns 10*. https://www.apple.com/newsroom/2018/07/app-store-turns-10/

Babaei, G., Giudici, P., Raffinetti, E. (2025). A Rank graduation box for S.A.F.E. AI. Expert systems with applications, 59, 125239.

European Commission. (2018). *General Data Protection Regulation (GDPR)*. https://gdpr.eu/

European Commission. (2022). *Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act)*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065

European Commission. (2022). *Regulation (EU) 2022/1925 on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R1925

European Commission. (2022). *Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act)*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454

European Commission. (2022). *Regulation (EU) 2022/868 on European Data Governance (Data Governance Act)*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868

European Commission. (2023). *Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0068

European Commission. (2024, February 6). *Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689*. Retrieved from Commission Publication Platform. Artificial Intelligence Act

European Commission. (2025, February 6). *Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689*. Retrieved from Commission Publication Platform. Artificial Intelligence Act+1

European Commission. (2023). *eIDAS 2.0 Regulation*. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

European Commission. (2024). *Artificial Intelligence Act (EU Regulation 2024/1689)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

European Commission. (2024). *EU Cybersecurity Act: Regulation (EU) 2019/881 (updated certification framework)*. Official Journal of the European Union. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

European Commission. (n.d.). *Architecture Reference Framework for the eIDAS Nodes*. https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Architecture+Reference+Framework

European Parliament & Council of the European Union. (2024, April 11). *Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

European Parliament & Council of the European Union. (2024, June 13). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (the EU AI Act)*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj wiz.io+15Artificial Intelligence Act+15NIST Publications+15EUR-Lex+2Artificial Intelligence Act+2

Froomkin, A. M. (2003). *Addressing Online Identity: Understanding the Microsoft Passport Service*. ResearchGate. https://www.researchgate.net/publication/293555641_Addressing_Online_Identity_Understanding_the_Microsoft_Passport_Service

Good Health Pass Collaborative. (2021). https://www.goodhealthpass.org/

Government of Slovenia. (2023). *European Digital Identity Wallet (EUDI)*. https://www.eudiwallet.gov.si/en/about-the-project/self-sovereign-identity/

Heath, A. (2019). *The Oral History of Amazon Prime*. Vox. https://www.vox.com/recode/2019/5/3/18511544/amazon-prime-oral-history-jeff-bezos-one-day-shipping

ID2020 Alliance. (2016). https://id2020.org/

INATBA. (2024). *AI Regulation and Blockchain: Bridging Ethics and Governance*. International Association for Trusted Blockchain Applications (INATBA). https://inatba.org/policy/ai-regulation-and-blockchain-bridging-ethics-and-governance/

INATBA. (2025). *Blockchain as an Enabler of Trusted AI – AI & Blockchain Convergences Task Force Report*. https://inatba.org/publications/blockchain-as-an-enabler-of-trusted-ai/

International Organization for Standardization/International Electrotechnical Commission. (2023). *ISO/IEC 23894:2023 — Information technology — Artificial intelligence — Guidance on risk management*. https://www.iso.org/standard/77304.html

International Organization for Standardization/International Electrotechnical Commission. (2022). *ISO/IEC 38507:2022 — Governance implications of the use of artificial intelligence by organizations*. https://www.iso.org/standard/56641.html

International Organization for Standardization/International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 — Information security management systems*. https://www.iso.org/isoiec-27001-information-security.html

International Organization for Standardization/International Electrotechnical Commission. (2011). *ISO/IEC 25010:2011 — Systems and software quality models*. https://www.iso.org/standard/35733.html

International Organization for Standardization/International Electrotechnical Commission. (2015). *ISO 9001:2015 — Quality management systems — Requirements*. https://www.iso.org/iso-9001-quality-management.html

International Organization for Standardization/International Electrotechnical Commission. (2012). *ISO/IEC 24760-1:2012 — Identity management framework, Part 1: Terminology and concepts*. https://www.iso.org/standard/57914.html

Iqbal, M., Alam, F., Nasir, Q., & Mahmod, R. (2024). *Blockchain-based Self-Sovereign Identity: A Systematic Mapping Study*. *Heliyon*. https://www.sciencedirect.com/science/article/pii/S2405844024141680

Islam, M. M. (2021). *A Review of LDAP and Its Application in Enterprise Systems*. *KnE Engineering*. https://kneopen.com/KnE-Engineering/article/view/3652

Kiva Protocol. (n.d.). *Digital Identification for Financial Inclusion*. https://www.kiva.org/protocol

Kosinski, M., Stillwell, D., & Graepel, T. (2013). *Private traits and attributes are predictable from digital records of human behavior*. *PNAS*. https://pubmed.ncbi.nlm.nih.gov/23479631/

Microsoft. (n.d.). *ION: A Decentralized Identifier Network*. GitHub. https://github.com/decentralized-identity/ion

MOSIP. (2018). *Modular Open Source Identity Platform*. https://www.mosip.io/

National Institute of Standards and Technology. (2023, January 26). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. U.S. Department of Commerce. https://www.nist.gov/itl/ai-risk-management-framework WilmerHale+6NIST+6NIST Publications+6

National Institute of Standards and Technology. (2024, July 26). *NIST AI RMF Generative AI Profile (NIST AI-600-1)*. U.S. Department of Commerce. https://www.nist.gov/itl/ai-risk-management-framework Reuters+8NIST+8WilmerHale+8

Nicas, J. (2020). *Google's Ad Dominance Sets Off an Antitrust Alarm*. *The New York Times*. https://www.nytimes.com/2020/09/21/technology/google-doubleclick-antitrust-ads.html

OAuth. (2023). *OAuth 2.0 Authorization Framework*. https://oauth.net/2/

Polygon ID. (n.d.). *Polygon ID Tutorials – Identity Infrastructure for Web3*. https://0xpolygonid.github.io/tutorials

Rahman, S., et al. (2023). *Framing Digital Identity as a Societal Asset: New Policy Imperatives*. *Sage Journals*. https://journals.sagepub.com/doi/10.1177/20438692312002 86

Sovrin Foundation. (n.d.). *Sovrin Protocol and Glossary*. https://sovrin.org/library/sovrin-protocol-and-glossary/

The Economic Times. (2023, November 22). *Aadhaar data leak: Personal data of 81.5 crore Indians on sale on dark web: Report*. https://economictimes.indiatimes.com/tech/technology/aadhar-data-leak-personal-data-of-81-5-crore-indians-on-sale-on-dark-web-report/articleshow/104856898.cms?from=mdr

Trinsic. (n.d.). *Trinsic Blog – Building the Identity Layer of the Internet*. https://trinsic.id/blog/

Uddin, M. M., et al. (2023). *Zero Knowledge Proofs: A Comprehensive Review of Applications, Protocols, and Future Directions in Cybersecurity*. *ResearchGate*. https://www.researchgate.net/publication/373097436_Zero_Knowledge_Proofs_A_Comprehensive_Review_of_Applications_Protocols_and_Future_Directions_in_Cybersecurity

United Nations. (2015). *Transforming our world: The 2030 agenda for sustainable development (A/RES/70/1).* United Nations General Assembly. https://sdgs.un.org/2030agenda

United Nations Educational, Scientific, and Cultural Organization. (2021). *Recommendation on the ethics of artificial intelligence*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000380455

United Nations Educational, Scientific, and Cultural Organization. (2019). *UNESCO's approach to digital inclusion: Fostering access to information and knowledge for all*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000368962

United Nations Educational, Scientific, and Cultural Organization. (2022). *Reimagining our futures together: A new social contract for education*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000379707

United Nations Educational, Scientific, and Cultural Organization. (2023). *Culture 2030 indicators: Linking culture to the United Nations Sustainable Development Goals*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000371562

W3C. (2021). *Verifiable Credentials Data Model v1.1*. https://www.w3.org/TR/vc-data-model/

W3C. (2022). *Decentralized Identifiers (DID) v1.0*. https://www.w3.org/TR/did-core/

World Bank. (2023). *Identification for Development (ID4D)*. https://id4d.worldbank.org/

World Economic Forum. (2018). *A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity*. https://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf Also available at: https://www.weforum.org/reports/a-blueprint-for-digital-identity

World Wide Web Consortium. (2019). *Decentralized Identifiers (DIDs) v1.0*. https://www.w3.org/TR/did-core

World Wide Web Consortium. (2019). *Verifiable Credentials Data Model v1.1*. https://www.w3.org/TR/vc-data-model

Zubair, F. (2023). *Single Sign-On with SAML and Its Implementation*. *ResearchGate*. https://www.researchgate.net/publication/383943912_Single_sign_ON_with_SAML_and_its_Implementation

11. Annex

11.1. Evidence-Friendly Architecture and Implementation Framework

E.1 Reference Architecture: SSI–AI–DLT Integration

This reference architecture defines how Self-Sovereign Identity (SSI), Artificial Intelligence (AI), and Distributed Ledger Technologies (DLT) interact in a **verifiable, auditable, and interoperable** manner.

Core Components:

1. **Issuer**: An authorized entity issues a Verifiable Credential (VC) — e.g., JSON-LD VC 2.0 or ISO mDoc — signed with BBS+/EdDSA.
2. **Holder/Wallet**: User-controlled, EUDI-compliant wallet; communicates securely via DIDComm v2.
3. **Verifier/Service**: Issues a proof request (Presentation Definition) with a Zero-Knowledge (ZK) policy.
4. **AI Decision Module**:
   - **Input**: Selectively disclosed attributes + ZK proofs.
   - **Runtime**: Executed within TEE/Confidential VM; model card and data source documentation attached.
   - **Output**: Produces a **Signed Inference Token (SIT)**.
5. **Ledger/Trust Registry**: Maintains issuer lists, revocation/status registries, and policy identifiers.
6. **Audit/Provenance Layer**: Stores SIT, credential hashes, and minimal transaction metadata.

Data Flow:
Issuer → VC → Holder → ZK/Selective Disclosure → Verifier + AI → SIT → Ledger/Audit.

E.2 AI Act – SSI Applicability Matrix

Use Case	AI Act Risk Level	Required SSI Artifact	Evidence/Log	Privacy Technique	Revocation
Remote biometric verification	High	VC: KYC-assertion + liveness attestation	Decision log + SIT	TEE + DP (ε\varepsilonε), ZK-age proof	Status List 2021

Credit/eligibility scoring	High	Income/employment VCs	Model version + feature provenance	DP + federated learning	Model rollback
Age verification	Limited	ZK-DoB proof (≥18)	Minimal log	zk-SNARK/BBS+ SD	Automatic
Content moderation	Limited	Role VC	Policy-bound explanations	C2PA provenance	N/A

Signed Inference Token (SIT): A cryptographically signed object summarizing which VCs and model version were used, under which policy, to produce the decision.

E.3 Threat Model and Mitigation Controls (STRIDE adaptation)

Threat	Example	Mitigation Control
Identity spoofing	Stolen VC / QR replay	Nonce + holder binding; liveness proof
Privilege escalation	Delegation chain abuse	Delegation VC + scope/time constraints
Correlation risk	Multi-presentation linkage	BBS+ SD, pairwise DIDs
Model bias	Data distribution shift	Fairness KPIs + drift detection
Data leakage	Reverse inference from features	DP, TEE, feature clipping
Phishing/verifier impersonation	Fake verifier endpoint	Trust registry + verifier attestation

E.4 Performance and Security Metrics (for Pilots)

- **Privacy**: Average disclosed fields / requested fields; ε\varepsilonε range.
- **Fairness**: |TPRgroupA−TPRgroupB||TPR_{groupA} - TPR_{groupB}||TPRgroupA−TPRgroupB| difference.
- **Reliability**: Revocation propagation time (t_revoke), FAR/FRR rates.
- **User Experience**: Proof presentation, P95 latency, abandonment rate.

- **Governance**: Average response time to audit requests.

E.5 Standards and Interoperability Mapping

Requirement	Standard
VC format	W3C VC 2.0 / ISO 18013-5
Communication	DIDComm v2, OpenID4VP/4VCI
Signature/Disclosure	BBS+ SD-JWT / SD-JWT VC
Revocation	Status List 2021
Trust registry	OID-Fed / EBSI Trust List
Provenance	C2PA/Content Credentials
Secure execution	TEE/Confidential Computing

E.6 "Verifiable Inference" Design Pattern

1. **Input Evidence**: Digest of presented VCs, revocation status snapshot ID.
2. **Execution Context**: Model version hash + TEE attestation quote.
3. **Output**: SIT (model_id, policy_id, inputs_digest, decision, explanation_pointer, timestamp).
4. **Explainability**: Policy-bound XAI — disclose only the n most influential causal features + counterfactual recommendation.
5. **Privacy**: Feature-level differential privacy; explanation-level k-anonymity.

E.7 Mini Case Studies

1. **DeFi KYC-lite**: Exchange requests a KYC VC asserting "PEP/SDN-free" status + proof-of-residency → holder presents via ZK → AI fraud score computed → SIT signed → auditable in compliance review.
2. **Cross-border diploma verification**: University issues VC → employer verification → AI profile matching with provenance logging.
3. **IoT/EV charging station authorization**: Station requests device VC + operator role VC → AI anomaly detection → revocation propagated instantly.

11.2. Glossary of Technical Terms

AI Applied to SSI

Adversarial Testing / Red Teaming: Offensive testing to uncover failures, jailbreaks, and biases.

Bias / Fairness: Model biases and equity; require explicit metrics and mitigations.

Federated Learning: Train models without moving raw data; share gradients/updates instead.

Guardrails / Policy Engine: Policies as code that control inputs, outputs, and allowed purposes.

Model Card / Data Card: Documentation of purpose, training, metrics, limits, and risks.

RLHF / RLAIF: Fine-tuning with human or AI feedback to align behaviors.

XAI (Explainable AI): Methods to explain model decisions. Why it matters: regulation and UX.

Architecture and Operations

Golden Path / Reference Architecture: Preferred route and reference design to deliver use cases with lower risk.

Multichain Interoperability: Operate across multiple ledgers/networks without rebuilding the stack.

Observability (Logs/Metrics/Traces): Telemetry to detect incidents, model drift, and compliance issues.

Off-chain / On-chain: Personal data off-chain; proofs/statuses on-chain. Default safe pattern.

Kill-Switch (Credential/Model): Standardized mechanism to disable a credential or a model during incidents.

Policy as Code: Executable, versioned policies (e.g., OPA/Rego) for auditable enforcement.

Policy Registry / Governance Registry: Signed and versioned repositories of policies and authorities.

Rollback Plan: Procedure to revert to a trusted state after failures or faulty updates.

Runtime Attestation: Continuous verification of service integrity.

SLO/SLA: Service level objectives/agreements (availability, latency, revocation within X minutes).

Zero Trust: “Never trust, always verify” security model for agents and APIs.

Cryptography and Security

Attestation: Signed evidence that a component (software/hardware) is intact and genuine.

Audit Log / Ledger: Immutable event log (signatures, revocations, policy changes).

BBS+ / CL Signatures: Signature schemes enabling selective disclosure and unlinkability.

CVM (Confidential VM): Virtual machines with encrypted memory and protected state.

KMS (Key Management Service): Service to store and rotate cryptographic keys.

MPC (Multi-Party Computation): Joint computation on private inputs without revealing them.

PQC (Post-Quantum Cryptography): Cryptography resistant to quantum attacks; hybrid PQC combines PQC with classical schemes.

TEE / Enclaves (Trusted Execution Environment): Hardware-isolated secure execution environment.

ZKP (Zero-Knowledge Proof): Prove a statement without revealing the underlying data (e.g., “over 18” without the birthdate).

Data, Privacy, and Compliance

Consent Management: Recording and managing user consent (granular and revocable).

Data Minimization: Collect and process only what is necessary.

Differential Privacy: Statistical noise to protect individuals in aggregated datasets.

DPIA (Data Protection Impact Assessment): Assessment for high-risk processing activities.

GDPR / eIDAS 2.0 / EU AI Act: European frameworks for data protection, identity, and AI risk management.

Provenance (of data/models): Traceability of origin, transformations, and usage.

Pseudonymization / Anonymization: Techniques to reduce identifiability; not equivalent and don’t guarantee the same protections.

Purpose Limitation: Use data only for the consented purpose.

Decentralized Identity (SSI)

Binding (Account/Device/Identity Binding): Methods to link a DID to a person or device (cryptographic/biometric).

Decentralized Biometrics: On-device/edge biometric verification without centralizing raw templates.

DID (Decentralized Identifier): Verifiable, resolvable identifier (e.g., did:method:123...) anchored to a network.

DID Document: Metadata associated with a DID (public keys, endpoints, verification methods).

Holder / Issuer / Verifier: Core roles: the subject who presents (Holder), the authority that attests (Issuer), and the relying party that validates (Verifier).

Revocation / Status List: Mechanisms to invalidate or check the status of credentials (loss, expiry, fraud).

Schema / Credential Definition: Data structure and rules for issuing/validating a credential type.

Selective Disclosure: Revealing only the minimum necessary fields from a credential. Why it matters: minimizes exposure.

SSI (Self-Sovereign Identity): A Model where people and organizations control their identity and credentials without relying on a single provider. Why it matters: reduces lock-in and improves privacy.

Trust Registry: Registry of authorized issuers/verifiers and associated policies.

VC (Verifiable Credential): Signed claim about a subject (e.g., professional license) with cryptographic proofs.

VP (Verifiable Presentation): A Package of one or more VCs presented to a verifier with proof.

Wallet (SSI Wallet): Application that manages DIDs, VCs, keys, and consent.

Protocols and Standards

DIDComm v2: Secure peer-to-peer messaging between SSI agents (offers, requests, presentations).

OpenID4VC / OIDC4VP: Extensions of OpenID Connect for issuing and presenting verifiable credentials.

OIDC / OAuth 2.0: Widely used Web2 authentication/authorization protocols; connect to SSI via OIDC bridges.

Presentation Exchange: Standard for verifiers to express exactly which proofs they require.

SiOP (Self-Issued OpenID Provider): The user acts as their own OpenID Provider via a wallet.

W3C VC Data Model: Core specification for VC format and proofs.

Product and UX

Consent UX: Clear interface for granting/withdrawing consent (including expiry and purpose).

Progressive Disclosure: UI guiding users to reveal only the minimum necessary data.

Risk-Based UX: Variable friction based on risk (more checks for higher-risk scenarios).

Verifiable Receipts: Signed receipts of what was presented/accepted for user-side auditability.

Use Cases (mental shortcuts)

Access to Critical Infrastructure: Physical/digital access control with policy-as-code and fast revocation.

Benefits Eligibility: Selective proofs (income, residence) without exposing raw data.

Licensing/Registration: Issuance and validation of professional licenses across borders.

Verifiable KYC/AML: Client onboarding with VCs + ZKPs, revocation, and audit.

Contact details

Website inatba.org

Contact contact@inatba.org

Join INATBA membership@inatba.org