eBook

Rebuilding Digital Trust

A Strategic Guide to Self-Sovereign Identity for Regulated Industries

Cardano Foundation

Why traditional identity systems are under strain

Cyber threats, compliance complexity, and rising user distrust are converging—especially in heavily regulated industries—to force a modernization of enterprise identity management.

80%

of cyberattacks today are identity-based[2]

93%

of organizations endured two or more identity-related breaches in the past year[3]

Traditional identity is failing to meet modern enterprise needs.

Centralized and federated identity models create bottlenecks, limit user control, and fragment systems—driving identity sprawl, inconsistent policies, and poor visibility that weaken governance and security.[1]

Self-sovereign identity offers a privacy-first alternative to legacy IAM.

Self-sovereign identity uses portable, user-controlled credentials on open standards, enabling consent-based sharing, stronger privacy, and reduced reliance on intermediaries—offering a credible, regulation-aligned alternative to legacy IAM.

Identity-related breaches continue to be a critical threat to regulated industries.

Healthcare, finance, insurance, and telecom face rising identity-related breaches—driving 80% of cyberattacks. SSI mitigates risk by embedding trust directly into credential exchanges.

Real-world deployments demonstrate SSI's value across various sectors.

Healthcare, finance, and government use SSI for secure access, streamlined compliance, and cross-border verification—strengthening trust, reducing risk, and improving operational efficiency.

The identity crisis in regulated industries

Fragmented systems, redundant processes, and limited user control drive higher costs, increased risk, and reduced trust in traditional identity approaches.

Core challenges undermining enterprise identity management

Duplicate KYC and credentialing processes

Repeated KYC checks across departments waste time, increase costs, and cause inconsistent records due to disconnected verification workflows.

Redundant or siloed identity repositories

Multiple unconnected identity stores raise management costs, create inconsistencies, and expand the attack surface for potential breaches.

High compliance and verification overhead

Evolving regulations necessitate costly, labor-intensive verification and audit processes that strain resources and impede operational efficiency.

Poor user control and lack of data portability

Users cannot easily manage, move, or selectively share identity data, creating friction and reducing trust across platforms.

Finance

Global financial institutions spend up to $60 million annually per firm on KYC and onboarding costs.[4] Meanwhile, fraud continues to rise, costing the sector over $30 billion each year.[5]

Healthcare

Over 30% of healthcare spending is administrative, with a significant portion tied to identity verification, access control, and credentialing.[6]

Supply Chain

Regulatory and compliance documentation inefficiencies cost the global supply chain industry over $1.85 trillion annually, with identity fraud and counterfeit documentation as major contributors.[7]

Exploring identity management infrastructure

Modern enterprises operate across multiple platforms, partners, and jurisdictions. Identity management systems must therefore be resilient, interoperable, and privacy-preserving.

Why centralized and federated models fall short of modern enterprise needs.

Both models concentrate trust in a limited set of actors, creating security, compliance, and user-experience challenges that become more acute as regulatory pressure and cyber threats grow.

Centralized Identity

Relies on a single provider to store and manage all identity data. It simplifies internal control and policy enforcement, but creates a single point of failure, limits interoperability, and offers users minimal visibility or control over their data.

Federated Identity

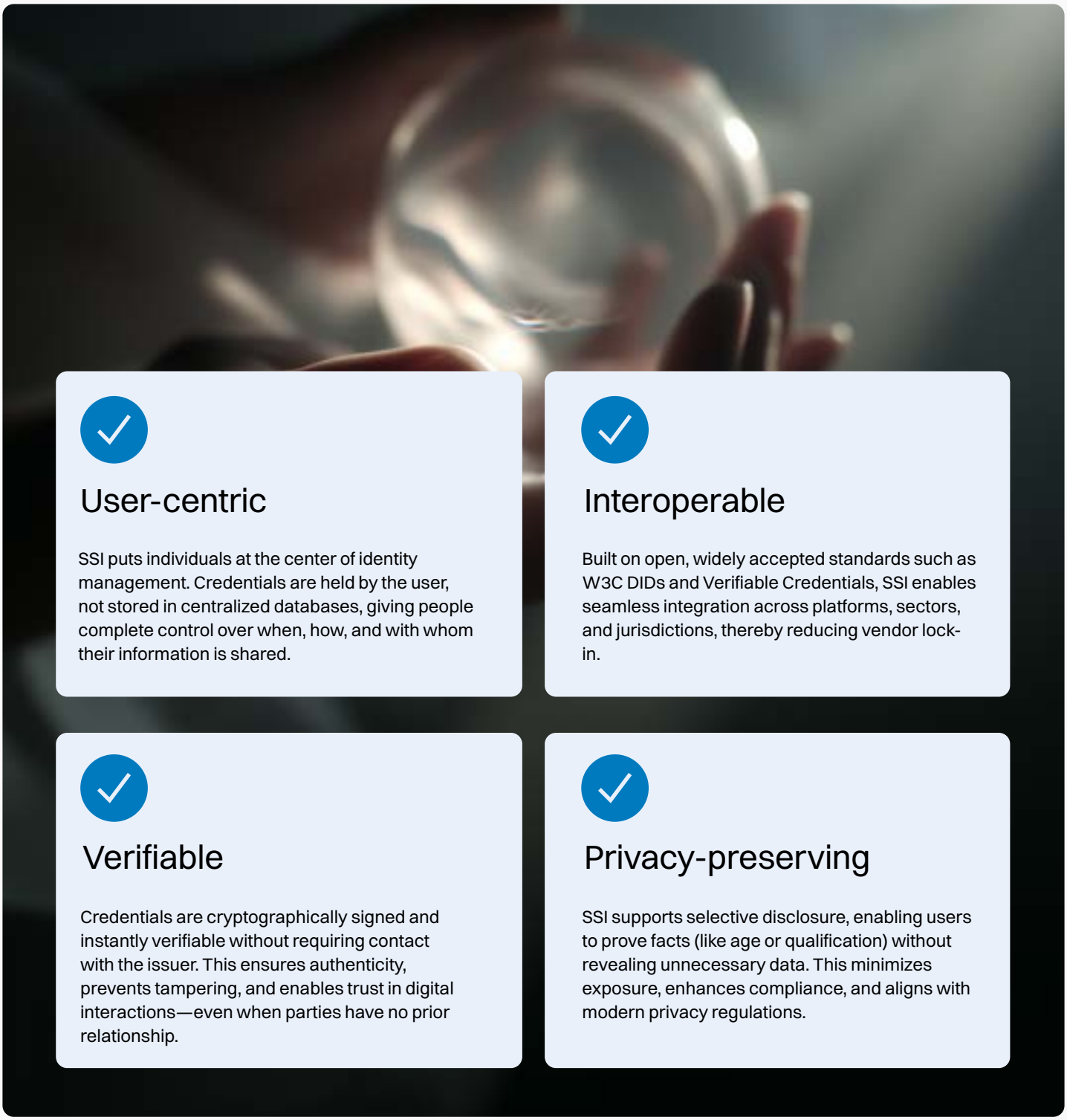
Enables users to access multiple systems using one credential, typically managed by a third-party intermediary. It improves usability and reduces login friction, but concentrates trust, raises privacy concerns, and limits user control and data portability.

Self-Sovereign Identity

Allows users to hold and present portable, verifiable credentials issued by trusted entities. It enhances privacy, control, and interoperability, but depends on emerging standards, shared governance, and broad ecosystem adoption to reach full enterprise maturity.

Core principles of self-sovereign identity

SSI is a digital identity model in which individuals and organizations own and manage their identity data. Identity-related claims are issued as verifiable credentials that can be cryptographically verified without requiring contact with the issuer.



User-centric

SSI puts individuals at the center of identity management. Credentials are held by the user, not stored in centralized databases, giving people complete control over when, how, and with whom their information is shared.

Interoperable

Built on open, widely accepted standards such as W3C DIDs and Verifiable Credentials, SSI enables seamless integration across platforms, sectors, and jurisdictions, thereby reducing vendor lock-in.

Verifiable

Credentials are cryptographically signed and instantly verifiable without requiring contact with the issuer. This ensures authenticity, prevents tampering, and enables trust in digital interactions—even when parties have no prior relationship.

Privacy-preserving

SSI supports selective disclosure, enabling users to prove facts (like age or qualification) without revealing unnecessary data. This minimizes exposure, enhances compliance, and aligns with modern privacy regulations.

Key technologies behind self-sovereign identity

SSI is made possible by a set of core technologies that work together to enable secure, privacy-respecting, and interoperable digital identity. These building blocks, built on open standards, shift control from centralized authorities to the individual, while ensuring verifiability and trust at scale.

Decentralized Identifiers (DIDs)	DIDs are globally unique, standards-based identifiers created and managed by users without reliance on centralized registries. They serve as the foundation for user-controlled identity, enabling secure, persistent references to individuals, organizations, or devices across digital ecosystems.
Verifiable Credentials (VCs)	VCs are digitally signed credentials issued by trusted entities—such as governments, banks, or employers—that can be verified without requiring contact with the issuer. They support granular data sharing, cryptographic authenticity, and tamper resistance, while protecting user privacy.
Digital Wallets	Digital wallets enable individuals to store, manage, and share verifiable credentials under their control. With built-in consent mechanisms, they allow users to selectively disclose identity data when needed, securely and without relying on third-party platforms.
Zero-Knowledge Proofs (ZKPs)	ZKPs enable users to prove something is true—such as their age or income level—without revealing the actual data. This privacy-enhancing technique helps reduce data exposure while maintaining trust in high-assurance identity verification processes.
Trust Frameworks	Trust frameworks define the rules, credential schemas, roles, and governance models that underpin SSI ecosystems. Examples like eIDAS 2.0 or GLEIF's vLEI ensure that verifiable credentials are recognized, auditable, and revocable within regulated and cross-border environments.

Self-sovereign identity in action

The principles of decentralized identity extend beyond securing IoT devices to solve complex challenges for people and businesses across multiple sectors. This model allows individuals and organizations to control their data while enabling trusted, secure, and efficient interactions. The same cryptographically verifiable credentials that secure machines are now a powerful tool in a wide range of industries, from finance to healthcare and beyond.

Banking and finance

SSI reduces onboarding costs with reusable KYC credentials and enables real-time verification that supports AML compliance, mitigates fraud, and accelerates customer acquisition across digital channels.

Healthcare

SSI improves patient access, consent management, and clinician credentialing, while enhancing care delivery and ensuring compliance with regulations like HIPAA and GDPR.

Supply chain

SSI powers digital product passports, supplier certifications, and tamper-proof proof of origin—enabling trusted ESG and compliance documentation across global supply networks.

Government services

Mandates like eIDAS 2.0 drive the adoption of digital identity wallets, enabling secure, cross-border access to public services for citizens and businesses.

Navigating the global regulatory environment

Self-Sovereign Identity (SSI) is no longer a fringe innovation—it is gaining regulatory momentum worldwide. Governments and standards bodies are formalizing the implementation of verifiable credentials, digital wallets, and decentralized identifiers to ensure trust, interoperability, and legal recognition at scale.

eIDAS 2.0

The revised eIDAS 2.0 regulation requires all EU member states to offer government-recognized Digital Identity Wallets by 2026. These wallets will enable citizens and businesses to access both public and private services securely across borders using verifiable credentials.

ISO/IEC 18013-5 and 27560

These international standards define the processes for issuing, storing, and presenting mobile driving licenses and verifiable credentials. They lay the foundation for interoperable, privacy-preserving digital ID across government and commercial use cases, supporting global trust and adoption of SSI.

GLEIF vLEI

The vLEI framework delivers verifiable digital credentials that confirm a legal entity's identity and its authorized representatives. This enhances transparency, simplifies onboarding, and supports global regulatory compliance in sectors such as finance, supply chain management, and legal services.

Over 30% of enterprises are expected to adopt decentralized identity standards in compliance or onboarding workflows by 2026, signaling a shift toward user-centric and interoperable identity models.[8]

Strategic benefits for enterprises

Enterprises that adopt SSI frameworks report significant improvements in operational efficiency, user experience, security, and compliance.

Accelerated onboarding

Reusable credentials reduce redundant verification steps, cutting onboarding times by up to 70% in high-assurance industries.[9]

Fraud prevention

Cryptographically verifiable credentials reduce the risk of synthetic identities and unauthorized access, thereby enhancing security without introducing additional friction.

Compliance efficiency

Verifiable proofs streamline audit trails, reducing reliance on manual checks and enhancing readiness for regulations such as AML, HIPAA, and GDPR.

Customer experience

One-click identity verification and no password resets eliminate friction, improving satisfaction and reducing abandonment during digital onboarding.

Infrastructure future-proofing

Built on open standards and aligned with zero-trust models, SSI supports long-term scalability, privacy requirements, and vendor-neutral integrations.

Cost savings

Reducing identity verification duplication, breach exposure, and compliance overhead translates into lower operational costs across multiple business units.

SSI is foundational to digital trust, which is emerging as the next frontier of competitive advantage in the digital economy.[10]

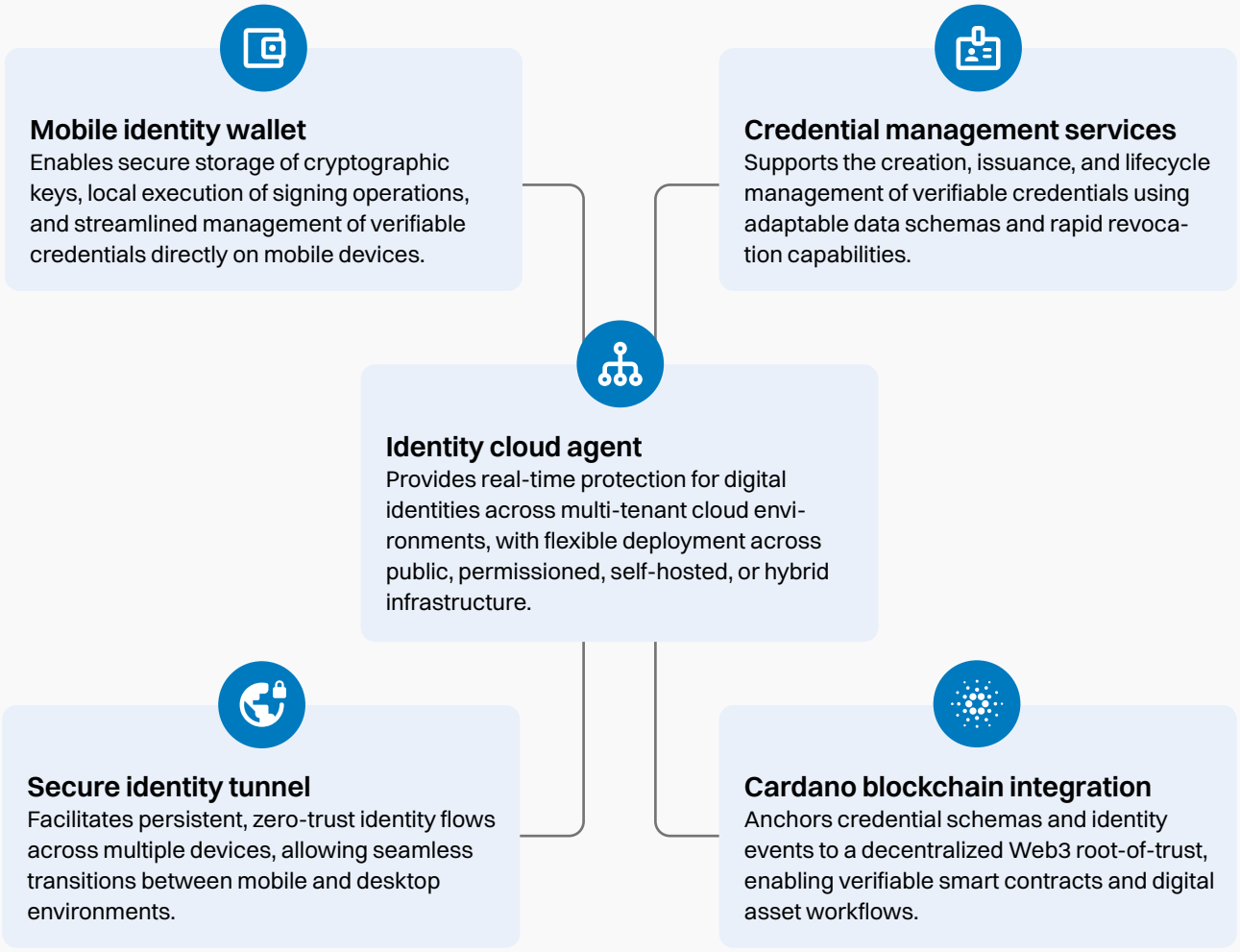
Veridian

The identity platform built for tomorrow

As the need for decentralized identity grows across regulated sectors, enterprises and governments are seeking practical and compliant solutions.

Veridian is the Cardano Foundation's open-source, enterprise-ready identity infrastructure, designed for compliance, scalability, and interoperability. It establishes a foundational layer of trust for regulated industries, enabling secure and verifiable data exchange across ecosystems such as finance, healthcare, and supply chains.

Secure digital identity management



Using the Cardano blockchain to support trusted digital interactions

Building digital trust is crucial for humanitarian aid to scale effectively, ensuring support reaches those who need it most. This case study explores how the UNDP Tadamon Accelerator leveraged the Cardano blockchain to create a system for issuing trusted, verifiable credentials to Civil Society Organizations (CSOs) worldwide.

The need for universally verifiable credentials

The Tadamon Accelerator for Food Security, led by UNDP, faced growing challenges verifying the legitimacy of CSOs across 57 member countries. Manual processes, inconsistent approvals, and unverifiable digital records created barriers to scale, transparency, and fraud prevention in delivering humanitarian support.

Scaling trust in Civil Society Organizations with Veridian

Tadamon partnered with the Cardano Foundation to launch a Proof of Concept using Veridian, a digital identity platform, to issue portable, verifiable credentials to CSOs. This blockchain-based system enhances trust, enables secure digital approvals, and creates a scalable model for future public sector verification and development programs.

Expanded reach

Tadamon aims to become the world's largest interactive CSO database by 2029.

Reduced fraud risk

Verifiable digital identity decreases impersonation and forgery.

Faster verification

On-chain records significantly reduce time and manual effort.

Full transparency

Immutable data supports real-time application monitoring.

Empowered CSOs

Verified credentials improve access to funding and partnerships.

Portable identity

DID-compliant credentials usable across platforms and programs

"We are confident that this partnership will strengthen our collective presence in OIC Member Countries and empower, inspire, and connect CSOs in their mission to improve the socio-economic well-being of marginalized communities."

Robert Pasicko
UNDP Program Coordinator

Sources

1 Gartner, The Emerging Architecture of Identity Management
2 CrowdStrike 2023 Threat Hunting Report
3 CyberArk 2024 Identity Security Threat Landscape
4 Thomson Reuters, Financial Institutions & Know Your Customer Rules
5 Thomson Reuter, 2023 Cost of Compliance
6 McKinsey & Company, Administrative Simpli cation: How to Save a Quarter-Trillion Dollars in U.S. Healthcare
7 PwC, Shifting Patterns: The Future of the Logistics Industry
8 Gartner's Decentralized Identity Forecast, 2023
9 Signicat, Digital reusable identity: What is it and how to use it
10 Boston Consulting Group, A Great Digital Identity Solution Is One You Can't See

---

Cardano Foundation

The Cardano Foundation is an independent, Swiss-based not-for-profit advancing Cardano as a public digital infrastructure across a wide range of industries.

Explore more

cardanofoundation.org

Dammstrasse 16 • 6300 Zug Switzerland