Davydov Petro

Review of the Publication:
“Self-Sovereign Identity-Based IAM in Enterprises”

Introduction

This publication explores the potential of the “Self-Sovereign Identity (SSI)” paradigm to enhance “Identity and Access Management (IAM)” systems in enterprise environments. The authors pose two central research questions:

- What are the requirements of IAM in enterprises?
- How can SSI help address these requirements?

The primary goal of the study is not only to classify IAM requirements but also to assess how SSI - a decentralized, cryptographically secure identity model - can improve existing IAM solutions. The authors develop a prototype SSI - based IAM system, demonstrate its functionality, and evaluate its effectiveness through expert interviews.

Methodology

The study is grounded in the “Design Science Research (DSR)” methodology, which combines engineering and behavioral approaches to create artifacts that solve real world problems. DSR consists of three phases:

- Relevance cycle - identifying the problem and research requirements
- Design cycle - building and testing the prototype
- Rigor cycle - validating scientific contribution and generalizing results

To gather data, the authors conducted:

- “Systematic Literature Review (SLR)” - a lot of articles, selecting some for in-depth analysis
- “Requirement coding” - the authors made code group selected on categories
- “Semi structured interviews” with experts, followed by lot’s thematic coding

Based on this analysis, the authors clustered IAM requirements into four overarching categories:

1) Security & Compliance
2) Operability
3) Technology
4) User

The prototype was built using “Hyperledger Aries Cloud Agent (ACA - Py)” and “Hyperledger Indy”, with the “Esatus AG” digital wallet. It includes processes for issuing, using, and revoking “Verifiable Credentials (VCs)”.

Results

The study demonstrates that the SSI - based prototype can meet requirements across all four IAM categories:

1. Security & Compliance
   - ✓ Use of “Zero-Knowledge Proofs (ZKPs)”
   - ✓ Verification without revealing full credentials
   - ✓ Credential revocation via blockchain registry

2. Operability
   - ✓ Automation of issuance and revocation
   - ✓ Fast onboarding and offboarding
   - ✓ Reduced workload for IT departments

3. Technology
   - ✓ Compatibility with OIDC/OAuth
   - ✓ Support for gradual integration
   - ✓ Use of standards (VC, VP, DID)

4. User
   - ✓ Passwordless authentication
   - ✓ User control over data disclosure
   - ✓ Transparency via digital wallet interface

Experts confirmed that SSI has the potential to improve IAM systems, especially in terms of security, manageability, and user experience. They also noted challenges such as technical terminology, reliance on network connectivity for revocation checks, and the absence of credential chaining.

Key Insights

1. *SSI enables least privilege enforcement via ZKPs*

This is critical for enterprise security. It allows for precise access control without exposing full credentials. This could be foundational for building flexible ABAC models.

2. *Blockchain - based VC revocation is a reliable offboarding mechanism*

This mechanism allows rapid deactivation of access when employees leave. This, as a practical tool for automating access lifecycle management, especially in high-turnover environments.

3. *SSI supports gradual integration with existing IAM systems*

The ability to use VP attributes in JSON Web Tokens for OAuth creates a bridge between legacy and modern systems. This is, as strategically important for migration without risking current infrastructure investments.

4. *SSI wallets provide transparency and user control*

Users can see who has requested their credentials and revoke access. This is vital for building trust in systems where privacy is paramount. In work, this could enhance GDPR compliance and user empowerment.

5. *Lack of credential chaining is a scalability limitation*

This insight is important as a challenge to address. In large organizations where credentials must be linked, this functionality is essential. This should be taken into account when assessing the readiness of SSI for deployment in the enterprise.

Conclusion

This paper makes a significant contribution to the research on “decentralized IAM systems". The authors classify the requirements of enterprise IAM and create a prototype that demonstrates the practical viability of SSI. They show that SSI can improve security, manageability, technological compatibility, and user experience.

Future research could be done in the following areas:

- Benchmarking SSI with traditional IAM platforms (e.g., Keycloak, Azure AD)
- Integrating SSI with Zero Trust and IoT
- Impact of passwordless authentication on user behavior
- Designing credential chains and scalable revocation models

If you are practicing in the development of security architecture, you should take this work into account in the direction of creating flexible, transparent, and automated access systems so that the created environment meets modern standards and needs.

Vocabulary

Self-Sovereign Identity (SSI)

A digital identity model in which individuals or organizations fully own and control their identity data without relying on centralized authorities. SSI enables users to manage credentials and selectively disclose information using cryptographic proofs.

Identity and Access Management (IAM)

A framework of policies and technologies for ensuring that the right individuals have appropriate access to technology resources. IAM systems manage digital identities, authentication, authorization, and access control.

Source: NIST SP 800-53, ISO/IEC 27001

Design Science Research (DSR)

A research methodology that focuses on the creation and evaluation of artifacts designed to solve identified problems. It combines rigor (scientific validation) with relevance (practical utility).

Systematic Literature Review (SLR)

A structured method for identifying, evaluating, and synthesizing existing research on a specific topic. It follows predefined protocols to ensure transparency and reproducibility.

Requirement Coding

A qualitative data analysis technique used to categorize and interpret textual data (e.g., interview transcripts, literature) into meaningful codes and themes. Often used in grounded theory and thematic analysis.

SourSemi-Structured Interviews

A qualitative research method involving guided conversations with open-ended questions. It allows flexibility in exploring topics while maintaining consistency across participants.

Hyperledger Aries Cloud Agent (ACA-Py)

An open-source Python-based agent framework for building SSI applications. It supports DIDComm messaging, credential exchange, and integration with Hyperledger Indy.

Hyperledger Indy

A distributed ledger purpose-built for decentralized identity. It supports verifiable credentials, DIDs, and privacy-preserving authentication mechanisms.

Verifiable Credentials (VCs)

A W3C standard for digital credentials that are cryptographically signed and can be verified without contacting the issuer. VCs support selective disclosure and privacy-preserving proofs.

Zero-Knowledge Proofs (ZKPs)

Cryptographic protocols that allow one party to prove to another that a statement is true without revealing any information beyond the validity of the statement.

Credential Revocation

The process of invalidating a previously issued credential to prevent its future use. In SSI, revocation is often managed via cryptographic registries on a blockchain.

Blockchain Registry

A decentralized ledger that records transactions or state changes (e.g., credential issuance, revocation) in a tamper-evident manner. Used in SSI to store public keys, schemas, and revocation data.

OIDC (OpenID Connect)

An identity layer built on top of OAuth 2.0 that enables clients to verify the identity of end-users based on authentication performed by an authorization server.

OAuth 2.0

An authorization framework that enables applications to obtain limited access to user accounts on an HTTP service, without exposing user credentials.

Source: IETF RFC 6749

VC (Verifiable Credential)

A digital statement issued by an entity (issuer) about a subject, cryptographically signed and verifiable. It contains claims and metadata.

Source: W3C Verifiable Credentials Data Model

VP (Verifiable Presentation)

A data structure that contains one or more verifiable credentials shared by a holder with a verifier. It supports selective disclosure and proof of possession.

Source: W3C Verifiable Credentials Data Model

DID (Decentralized Identifier)

A globally unique identifier that does not require a centralized registration authority. DIDs resolve to DID Documents containing public keys and service endpoints.

Source: W3C Decentralized Identifiers (DID) Specification v1.0

Transparency via Digital Wallet Interface

The ability for users to view, manage, and control their credentials, connections, and disclosures through a secure and user-friendly interface.

Source: UX Guidelines for SSI Wallets (e.g., Lissi, Trinsic, esatus)

JSON Web Tokens for OAuth

A compact, URL-safe means of representing claims to be transferred between two parties. JWTs are used in OAuth 2.0 as bearer tokens for access control.

Source: IETF RFC 7519; OAuth.net JWT Guide

GDPR (General Data Protection Regulation)

A regulation of the European Union (EU 2016/679) that governs the processing of personal data and protects the privacy rights of individuals. It mandates transparency, consent, data minimization, and accountability.

Source: Official GDPR Text - EUR-Lex

Benchmarking SSI with Zero Trust and IoT

An emerging research direction that evaluates how SSI principles (user-controlled identity, selective disclosure) can be integrated with Zero Trust architectures and IoT ecosystems to enhance security, scalability, and device-level trust.