Implementing EVM-Based Self-Sovereign Identity to Meet European Digital Identity Compliance for Decentralized Finance

Gintarė Košubienė[1] [0009-0001-8548-3253] and
Saulius Masteika[2] [0000-0002-1770-670X]

[1, 2] Vilnius University, Muitines 8, LT-44280 Kaunas, Lithuania, EU
gintare.kosubiene@knf.vu.lt, saulius.masteika@knf.vu.lt

Abstract. This paper presents an implementation of a Self-Sovereign Identity (SSI) framework using Ethereum-based standards to meet the technical requirements of the European Digital Identity (EUDI) Architecture Reference Framework (ARF). By leveraging ERC-734/ERC-735 standards, the proposed eSSI system enables decentralized key management, verifiable claims, and on-chain auditability. A case study on the Sepolia testnet demonstrates functional alignment with EUDI goals, while highlighting the need for enhanced privacy mechanisms such as zero-knowledge proofs for full compliance.

Keywords: digital identity, SSI, ERC-734/ERC-735, EUDI ARF

1 Introduction

Digital identity is rapidly becoming a foundational layer of the modern digital economy, enabling access to services, legal interactions, and regulatory compliance. As identity fraud, synthetic identities, and document forgery escalate—particularly with the rise of AI-generated deepfakes and falsified credentials—the urgency for secure, privacy-preserving, and verifiable identity systems has never been greater [1].

In response to these challenges, the European Union has been actively developing a common digital identity framework for a decade [2]. The culmination of these efforts is the European Digital Identity (EUDI) initiative, alongside its Architecture Reference Framework (ARF), which lays out technical design principles such as selective disclosure, minimal data use, cross-border interoperability, and robust auditability [3].

Meanwhile, innovation in the private sector is advancing at a significantly faster pace than the development of public infrastructure for EUDI such as the European Blockchain Services Infrastructure (EBSI). Public blockchains,

Copyright © Gintarė Košubienė, Saulius Masteika, 2025. Published by Vilnius University Press. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.
DOI: https://doi.org/10.15388/LMITT.2025.13

particularly those using the Ethereum Virtual Machine (EVM), have gained traction as flexible platforms for SSI, offering programmable smart contracts and broad ecosystem adoption [5]. Ethereum-based projects such as uPort pioneered on-chain identity management with decentralized key control and claim issuance, but also revealed challenges in privacy and scalability [22]. More recent solutions, like Privado ID (formerly Polygon ID), leverage zero-knowledge proofs to enhance privacy-preserving verifiability, further demonstrating the evolving capabilities of public chains in supporting regulatory-compliant digital identity [23]. Despite these advancements, none of the existing solutions have been explicitly designed to comply with the specific technical and regulatory requirements set out in the EUDI Architecture Reference Framework (ARF). This forms the basis of our central hypothesis.

Hypothesis: An EVM-compatible digital identity framework, built on SSI principles, can fulfill the requirements of the EUDI ARF when implemented for decentralized finance.

To investigate this, the paper reviews the principles of SSI (Section 2), compares key Ethereum identity standards and their alignment with EUDI (Section 3), and presents a case study of an implementation on the Ethereum Sepolia testnet (Section 4), demonstrating how open blockchain infrastructure can bridge the gap between SSI principles and EUDI requirements.

2 Self-Sovereign Identity (SSI) Principles and Their Technological Foundations

Self-Sovereign Identity (SSI) defines a decentralized and user-centric approach to digital identity management, where individuals retain full control over their credentials and personal data [6]. The conceptual foundation of SSI is based on ten core principles articulated by Christopher Allen—one of the pioneers of decentralized identity [6]. These principles (see Table 1) address both the ideological imperative of user autonomy and the technical challenge of implementing identity systems without central authority.

Each SSI principle can be mapped to a set of enabling technologies such as Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), etc. The mapping approach combined conceptual analysis of Allen's SSI principles

[6] with a review of enabling technologies and relevant standards EUDI ARF [5], W3C [7], OpenID [8] and others [9-15]. This ensured that the resulting mappings reflect both SSI's technical vision and the compliance demands of European digital identity initiatives.

Table 1. SSI Principles and Their Technological Foundation.

SSI principle	Description	Technologies	Standards by EUDI
Existence	Users must be able to exist in the digital world, without the need for a third party.	Decentralized Identifiers (DIDs)	W3C DID [7]
Control	Users must control their identity and how it is used, shared, or hidden.	Consent management, Selective Disclosure	OpenID4VP [8], W3C VC [7]
Access	Users must have full access to their identity data and claims, including records that indicate any changes associated with their identity.	Digital Wallets, Identity Agents	EUDI Wallet
Transparency	Identity systems and their algorithms must be open, auditable, and understandable.	Open-Source Frameworks, Auditable Smart Contracts	ESSIF [9]
Persistence	Identities should be long-lasting, ideally as long as the user wants. But users must also be able to delete them when desired.	Blockchain-based Registries, PKI, Revocation Mechanisms	DKMS [10]
Portability	Identities must be transferable between systems and platforms.	Interoperable Wallets, W3C-compliant Formats	W3C VC [7]
Interoper-ability	Identities should work across platforms and borders, ensuring usability in diverse, global digital environments.	DIDComm [11], JSON-LD [12], OIDC [13]	DIF [11], EUDI ARF Interfaces [5]
Consent	Users must give informed consent before any identity data is shared.	Zero-Knowledge Proofs	OpenID4VC [8]
Minimization	Only the minimum necessary data should be shared.	Selective Disclosure, Zero Knowledge Proofs	ISO/IEC 27551 [14], W3C VC [7]
Protection	Identities must be protected against tampering and misuse.	Encryption, DKMS, Biometric Factors	ETSI TS 119 312 [15]

The EUDI concept closely aligns with the core principles of Self-Sovereign Identity (SSI), as outlined in the technical standards of the EUDI Architecture Reference Framework (ARF) (see Table 1, last column). The following section explores relevant Ethereum Request for Comment (ERC) standards that serve as the technical bases for implementing SSI in a way that ensures compatibility with EUDI compliance.

3 Comparative Analysis of ERC Standards for EUDI Compliance

Ethereum offers a modular and extensible environment for implementing decentralized identity systems. Several ERC standards have been proposed and partially adopted to enable various components of Self-Sovereign Identity (SSI), including identity creation, key management, credential issuance, and revocation. This section presents a comparative evaluation of both established and emerging ERC standards based on their support for SSI features and alignment with the standards supported by European Digital Identity (EUDI).

ERC-725 / ERC-734 / ERC-735 [16-17] form a foundational trio for on-chain identity management: ERC-725 defines a proxy smart contract that acts as a digital identity controlled by one or more keys, ERC-734 manages the associated keys with varying purposes (management, action, etc.), ERC-735 enables storing verifiable claims (or attestations) about the identity, issued by third parties. Together, these standards support user control, on-chain auditability, and integration with trusted issuers. However, privacy limitations arise when claims are publicly accessible, and additional off-chain data handling is needed to meet GDPR and ARF privacy standards.

EIP-1056 (did:ethr) [18] introduces a lightweight registry-based Decentralized Identifier (DID) method fully aligned with W3C DID specifications. It enables DID ownership and control using Ethereum addresses, key rotation and delegation without requiring full contract deployment, off-chain DID resolution using standard DID documents. EIP-1056 supports SSI's portability and persistence goals while keeping minimal identity data on-chain, aligning well with the EUDI ARF's emphasis on privacy and interoperability.

ERC-780 [19] offers a global claims registry allowing third parties to issue attestations to any Ethereum address. It is efficient for public claims but

lacks selective disclosure mechanisms. Consequently, it is less suitable for privacy-sensitive credentials unless used with zero-knowledge or off-chain validation layers.

ERC-1484 [20] aggregates multiple Ethereum addresses under a single digital identity. This model facilitates identity portability and unified credential management, especially across different applications or key pairs. However, its adoption remains limited, and integration with broader standards such as DIDs and VCs is still evolving.

ERC-1812 [21] is an emerging standard for off-chain verifiable credentials that includes an on-chain revocation registry. Key features include: credential issuance using EIP-712 typed data, support for off-chain storage and selective disclosure, lightweight on-chain revocation checks via credential hashes. This architecture closely aligns with EUDI ARF's privacy and minimal disclosure principles while ensuring verifiability and auditability. It is especially suitable for systems requiring compliance with data protection regulations.

Table 2. Comparison of ERC Standards Alignment with SSI Principles and EUDI Requirements.

Standard	SSI Feature Support	EUDI Aligment
ERC-725/734/735	High (identity, key management, claims)	Strong (requires off-chain privacy support)
EIP-1056	High (DIDs, key delegation)	Strong (W3C DID compatibility)
ERC-780	Moderate (claims registry)	Week (no selective disclosure)
ERC-1484	Moderate (identity aggregation)	Moderate (experimental)
ERC-1812	Strong (VCs, off-chain privacy)	Strong (selective disclosure, ZK)

Based on the comparison in Table 2, EIP-1056 and ERC-1812 offer the most comprehensive support for SSI implementation in compliance with the EUDI. They enable decentralized key management, privacy-respecting credential issuance, and lightweight revocation mechanisms. Meanwhile, ERC-725/734/735 serve as a robust and flexible foundation for identity prototyping, particularly where on-chain execution, traceability, and compliance testing are required. Their smart contract-native structure makes them ideal for early-stage experimentation and integration with decentralized applications.

4 eSSI Implementation Based on ERC-734/ERC-735

Our European Self-Sovereign Identity (eSSI) system has been implemented using the ERC-734 and ERC-735 standards, chosen for their high SSI feature support and strong compatibility with EUDI framework (see Table 2). A high-level overview of the smart contracts' architecture is described in Figure 1.

As illustrated in Figure 1, the *eSSI*[1] smart contract functions as a deployment and management hub for digital identities and their associated wallets. It contains mappings to track the relationships between each identity and wallet, while also maintaining registries of trusted service providers (issuers) and the set of supported claim topics.

The *eIdentity*[2] smart contract, based on ERC-734 and ERC-735, represents the core component for managing decentralized identities. It provides interfaces for identity owners to manage authentication keys and maintain claim records. The *eClaimIssuer*[3] smart contract ensures that claims associated with an identity can be cryptographically validated and revoked. Claims—issued by external parties—capture information such as identity attributes or status, and are verifiable via digital signatures. Leveraging ERC-735, claims can be updated or revoked as needed, supporting dynamic identity states. For instance, a previously valid claim can be invalidated upon document expiration or regulatory changes, such as the wallet being added to a sanctions list.

By integrating these components, the system provides a scalable and secure digital identity infrastructure. It supports essential SSI features such as on-chain claim revocation, interoperability with decentralized applications (via claim topics), and potential compliance with the EUDI ARF.

5 Scenario Based Simulation

To validate the feasibility and scalability of our eSSI implementation, smart contracts were deployed on the Ethereum Sepolia Testnet, chosen for its high transaction volume and broad potential user base. Over 2,000 digital identities were programmatically deployed, and various claim issuance and revocation scenarios were tested—particularly involving sanction-based claim topics.

---

1 https://sepolia.etherscan.io/address/0xE2a385125BD3D3D62DAB37702984D517B9153b9c#code
2 https://sepolia.etherscan.io/address/0x75B94C3393D48cfF750687B8e532C1Fea28b2013#code
3 https://sepolia.etherscan.io/address/0x5bbf8f095312cf2cf54f8f5e7c9c035b22640ded#code

Figure 1. High-Level Smart Contracts Architecture of eSSI.

The simulation demonstrated that an ERC-734/735-based identity system can functionally align with both the foundational principles of SSI and the technical EUDI requirements. Identity owners were able to manage keys independently, and trusted issuers could add or revoke claims in real time. The system correctly manages claim changes enabling dynamic enforcement of trust relationships. For example, when an identity received a claim indicating a regulatory issue, that claim could be revoked, rendering the identity invalid for specific operations. The use of structured claim topics played a key role in facilitating interoperability, allowing decentralized applications to understand and process claims in a standardized way.

However, one major limitation observed during the simulation was the lack of privacy-preserving mechanisms. Since all claim data and interactions were recorded on-chain, the system does not yet address privacy requirements such as those outlined in GDPR or in the EUDI ARF itself. To advance toward production readiness, future versions must incorporate technologies like Zero-Knowledge Proofs (ZKPs) and off-chain data anchoring strategies to ensure selective disclosure and user consent-driven data sharing.

6 Conclusion

The proposed eSSI solution, based on ERC-734/ERC-735 standards, confirms that Ethereum-based SSI implementations can fulfill key EUDI ARF requirements in decentralized finance contexts. This identity system enables decentralized key management, verifiable claims, and on-chain auditability. However, further enhancements—especially privacy-preserving features—are necessary to reach production-readiness. This work outlines a viable, regulation-aware blueprint for digital identity systems built on public blockchain infrastructure.

Acknowledgments. The publication was prepared during the implementation of the project "Implementation of R&D activities, creating APV products by Deverium, UAB" (Project No. 02-020-K-0034). The project is co-financed by the European Union. Findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of Deverium, UAB.

References

[1] Zhang, C.J., Gill A.Q., Liu, B., Anwar, M.J. (2025), AI-based Identity Fraud Detection: A Systematic Review, https://doi.org/10.48550/arXiv.2501.09239 .

[2] Official Journal of the European Union, (2014), Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, http://data.europa.eu/eli/reg/2014/910/oj.

[3] European Commission, (2021), Architecture and Reference Framework, https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.8.0/architecture-and-reference-framework-main/, last accessed 2025-04-07.

[4] Biedermann, B., Scerri, M., Kozlova, V., Ellul, J. (2023), A Systematization of Knowledge: Connecting European Digital Identities with Web3. https://arxiv.org/pdf/2409.19032.

[5] Biedermann, B., Scerri, M., Kozlova, V., Ellul, J. (2025), Aggregating Digital Identities through Bridging. An Integration of Open Authentication Protocols for Web3 Identifiers. http://dx.doi.org/10.48550/arXiv.2501.13770.

[6] Allen, C. (2016), The Path to Self-Sovereign Identity, https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/, last accessed 2025-04-07.

[7] W3C, Verifiable Credentials Data Model v1.1, (2022), https://www.w3.org/TR/vc-data-model/, last accessed 2025-04-07.

[8] OpenID, (2022), Whitepaper of OpenID for Verifiable Credentials, https://openid.net/wordpress-content/uploads/2022/06/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials-V2_2022-06-23.pdf , last accessed 2025-04-07.

[9] The European Self-Sovereign Identity Framework Lab, (2019), SSI Standards Overview, https://tno-ssi-lab.github.io/standardisation-overview/, last accessed 2025-04-07.

[10] Reed, D, Law, J., Hardman, D., Lodder, M., (2019), DKMS (Decentralized Key Management System) Design and Architecture V4, https://github.com/hyperledger/indy-hipe/tree/49fcd78883d38babe9c95a4e1d150969797cffa2/design/dkms, last accessed 2025-04-07.

[11] Identity Foundation, DIDComm Messaging v2.x https://identity.foundation/didcomm-messaging/spec/, last accessed 2025-04-07.

[12] W3C JSON-LD Working Group, JSON for Linking Data, https://json-ld.org/, last accessed 2025-04-07.

[13] OpenID, How OpenID Connect (OIDC) Works, https://openid.net/developers/how-connect-works/, last accessed 2025-04-07.

[14] The International Organization for Standardization and the International Electrotechnical Commission, (2021), ISO/IEC 27551: Information security, cybersecurity and privacy protection — Requirements for attribute-based unlinkable entity authentication, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27551:ed-1:v1:en

[15] Electronic Signatures and Infrastructures Technical Committee, (2023) Cryptographic Suites, https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.04.03_60/ts_119312v010403p.pdf

[16] ERC-725 Identity Standard, https://erc725alliance.org/, last accessed 2025-04-07.

[17] Frozeman, F.G., (2017) ERC: Key Manager #734, https://github.com/ethereum/EIPs/issues/734, last accessed 2025-04-07.

[18] Ethereum Improvement Proposals, (2018), ERC-1056: Ethereum Lightweight Identity, https://eips.ethereum.org/EIPS/eip-1056 , last accessed 2025-04-07.

[19] Tortensson, J., (2017), ERC: Ethereum Claims Registry, https://github.com/ethereum/EIPs/issues/780 , last accessed 2025-04-07.
[20] Ethereum Improvement Proposals, (2018), ERC-1484: Digital Identity Aggregator https://eips.ethereum.org/EIPS/eip-1484, last accessed 2025-04-07.
[21] Ethereum Improvement Proposals, (2019), ERC-1812: Ethereum Verifiable Claims, https://eips.ethereum.org/EIPS/eip-1812, last accessed 2025-04-07.
[22] Goel, A., Rahulamathavan, Y., (2024), A Comparative Survey of Centralised and Decentralised Identity Management Systems: Analysing Scalability, Security, and Feasibility, https://doi.org/10.3390/fi17010001.
[23] Kaleido documentation, Privacy & Anonymity, https://docs.kaleido.io/kaleido-platform/full-stack/privacy/#privacy-solutions, last accessed 2025-04-07.