Privacy-Preserving Identity Verification Using Zero-Knowledge Proofs and Verifiable Credentials

Raluca-Ioana Purcăruș
National University of Science and Technology Politehnica Bucharest
Bucharest, Romania
ralucapurcarus@yahoo.com

Roberta Cristiana Popa
National University of Science and Technology Politehnica Bucharest
Bucharest, Romania
robertapopa2001@gmail.com

Alexandru Bratu
National University of Science and Technology Politehnica Bucharest
Bucharest, Romania
ing.bratu.alexandru@gmail.com

Florin Haralambie
National University of Science and Technology Politehnica Bucharest
Bucharest, Romania
florin.haralambie@upb.ro

***Abstract*—As digital identity becomes foundational in decentralized ecosystems, privacy concerns arise when individuals must disclose personal information for authentication. This paper proposes a standardized approach to identity verification using Verifiable Credentials (VCs) and Zero-Knowledge Proofs (ZKPs), allowing users to prove specific claims without revealing sensitive data. By combining the W3C VC data model with cryptographic ZKPs, the defined architecture ensures minimal disclosure, strong authentication, and interoperability across systems. This standardization effort outlines essential interfaces, credential formats, and verification workflows to support privacy-preserving digital identity in sectors such as eVoting, finance, and cross-border services.**

Keywords—digital identity, Verifiable Credentials, Zero-Knowledge Proofs, decentralized environments, digital authentication, eVoting.

I. Introduction

Digital identity verification is essential in online voting systems, financial applications, and decentralized platforms. However, current mechanisms often require over-disclosure of personal data, introducing security and privacy risks. Verifiable Credentials (VCs), as standardized by the W3C, provide a framework for issuing and verifying claims [1] and have been the focus of recent academic and technical surveys highlighting their potential and limitations [2]. When combined with Zero-Knowledge Proofs (ZKPs), VCs can support selective disclosure and minimal trust assumptions [3]. This article presents a standardization proposal for integrating ZKPs with VCs, enabling privacy-preserving identity verification while maintaining trust, scalability, and interoperability. The approach is applicable to a wide range of use cases, including eligibility verification in elections and privacy-preserving KYC (Know Your Customer) in decentralized finance (DeFi).

II. System Architecture Overview

The proposed system comprises three main actors: the Issuer, the Holder, and the Verifier. The Issuer provides a digitally signed VC containing user claims. The Holder stores the VC locally and generates a ZKP attesting to specific claims without revealing the credential itself. The Verifier receives the proof and verifies its correctness and origin using public parameters.

The architecture supports the following phases:

- Credential Issuance: The Issuer signs a JWT or JSON-LD credential with required claims.
- Proof Generation: The Holder inputs the credential data into a ZKP circuit (e.g., Circom [4]) to generate a Groth16 proof.
- Verification: The Verifier checks the ZKP and verifies the credential's issuer using a trusted DID (Decentralized Identifier) method.

This flow ensures that only the claim is revealed, not the underlying personal information input.

III. Standardization Proposal

To support widespread adoption and secure interoperability, the following standardization components are proposed:

A. Verifiable Credentials Schema

Standardize a core set of mandatory and optional fields relevant to use cases such as eligibility, age verification, and residency. Encourage extensibility for domain-specific scenarios while maintaining schema consistency.

B. Credential Encoding

Specify encoding conventions for both JWT and JSON-LD formats. Define how ZKP-compatible claims (e.g., numeric values instead of full birthdates) should be represented. Ensure encoding is compact and deterministic to support circuit reproducibility.

C. ZKP Circuit Interfaces

Define a standardized interface for Zero-Knowledge Proof circuits. This includes specifying accepted formats for private and public inputs, consistent use of cryptographic hashing (e.g., Poseidon), and expected outputs such as the proof, public signals, and any derived nullifier hashes. Include circuit metadata and versioning for cross-implementation compatibility.

D. Verification Interfaces

Standardize RESTful and gRPC APIs for off-chain verification, along with smart contract ABI interfaces for on-chain validation. The input specification should include the proof, public inputs, verifying key reference, and credential metadata. The response structure must indicate proof validity, issuer authenticity, and revocation status.

E. Cryptographic Suite

Recommend Groth16 zk-SNARKs over BN254 for efficient proof size and tooling availability. For hashing, Poseidon is preferred due to its zk-SNARK compatibility. Support elliptic curve keys such as ECDSA over P-256 and EdDSA over Ed25519 for digital signatures and DID documents.

F. Trust Management and DID Integration

Support various DID methods (did:key, did:web, did:ethr) for issuer identification [5], , consistent with the approaches evaluated in recent surveys [2]. Standardize trust anchor discovery mechanisms, including static lists or registry lookups. Define revocation approaches compatible with ZKPs, such as hash-based registries or Merkle tree accumulators.

G. Wallet and Interoperability Standards

Specify minimal requirements for mobile and desktop wallets capable of storing VCs and generating ZKPs. Encourage shared schemas and interfaces to enable interoperability across issuers, verifiers, and applications.

IV. Use Cases

Several use cases can benefit from this privacy-preserving identity framework. In eVoting systems, voters can prove their eligibility to vote without revealing their identities, helping to prevent fraud and preserve anonymity. A VC issued by a trusted authority can contain a claim such as "isEligibleToVote: true", and the voter can use a ZKP to prove this without disclosing their name, address, or national ID. For age verification, users can prove they meet minimum age requirements without disclosing their full birthdate or government-issued ID. In cross-border identity scenarios, individuals such as refugees can prove verified credentials issued by trusted authorities across jurisdictions. For DeFi applications, users can demonstrate KYC or jurisdictional compliance without submitting sensitive documents to the service provider.

V. Conclusions

This article proposes a foundational standard for integrating Zero-Knowledge Proofs with Verifiable Credentials to achieve privacy-preserving identity verification. The approach combines established cryptographic protocols with interoperable identity frameworks, offering a pathway to scalable, secure, and privacy-respecting digital authentication.

Future work includes support for zk-STARKs, standard mobile wallet interfaces, and cross-chain proof portability.

References

[1] "Verifiable Credentials Data Model v2.0," W3C Recommendation, 15 May 2025. [Online]. Available: https://www.w3.org/TR/vc-data-model/. [Accessed 27 June 2025].

[2] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista and M. Conti, "A Survey on Decentralized Identifiers and Verifiable Credentials," *IEEE Communications Surveys & Tutorials,* p. 1–1, 2025.

[3] R. Shashidhara, R. C. Nair and P. K. Panakalapati, "Promise of Zero-Knowledge Proofs (ZKPs) for BlockchainPrivacy and Security: Opportunities, Challenges, andFuture Directions," *Security and Privacy,* vol. 8, no. 1, p. e461, 2024.

[4] "https://docs.circom.io," [Online]. Available: https://docs.circom.io/. [Accessed 26 June 2025].

[5] "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, 19 July 2022. [Online]. Available: https://www.w3.org/TR/did-1.0/. [Accessed 26 June 2025].