INTISARI

Peningkatan insiden pelanggaran data dan pencurian identitas menegaskan perlunya sistem pengelolaan identitas digital yang kuat. Sistem identitas terdesentralisasi, khususnya *Self-Sovereign Identity* (SSI), menawarkan solusi menjanjikan dengan memungkinkan individu mengelola identitas digital mereka secara mandiri tanpa bergantung pada otoritas terpusat. Meskipun potensinya besar, adopsi SSI menghadapi tantangan, terutama karena kurangnya interoperabilitas di antara berbagai protokol pertukaran kredensial seperti Aries-DIDComm dan OpenID for Verifiable Credentials (OID4VC). Penelitian ini mengembangkan sistem SSI-CEPI (*Self-Sovereign Identity with Credential Exchange Protocol Interoperability*) yang mengintegrasikan protokol DIDComm dan OID4VC dalam arsitektur *multi-tenancy*, memungkinkan satu instansi server untuk melayani beberapa pengguna dengan tetap menjaga keamanan dan isolasi data. Sistem ini mendukung operasi kritis seperti autentikasi, penerbitan, verifikasi, dan pencabutan kredensial melalui abstraksi protokol yang memungkinkan pengguna memanfaatkan keunggulan dari setiap protokol tanpa perlu memahami perbedaan teknisnya. Hasil pengujian pada penelitian ini menunjukkan bahwa OID4VC unggul dalam efisiensi penerbitan kredensial berskala besar karena tidak memerlukan koneksi langsung, sementara Aries-DIDComm menawarkan keamanan yang lebih baik dalam verifikasi yang memerlukan koneksi terjamin. Format kredensial seperti SD-JWT mendukung *selective disclosure* untuk privasi yang lebih baik, sedangkan JWT menawarkan kecepatan untuk proses verifikasi sederhana. Dengan mengatasi tantangan interoperabilitas dan menyelaraskan kelebihan setiap protokol serta format kredensial, penelitian ini memperkuat ekosistem identitas digital yang aman, dapat diskalakan, dan inklusif.

Kata kunci : *Self-Sovereign Identity*, interoperabilitas, protokol pertukaran kredensial, identitas terdesentralisasi, Aries-DIDComm, OID4VC

ABSTRACT

The rising incidents of data breaches and identity theft highlight the urgent need for robust digital identity management systems. Self-Sovereign Identity (SSI) provides a promising decentralized approach, empowering individuals to manage their digital identities independently without relying on centralized authorities. However, SSI adoption faces challenges, particularly due to the lack of interoperability between credential exchange protocols such as Aries-DIDComm and OpenID for Verifiable Credentials (OID4VC). This study develops SSI-CEPI (Self-Sovereign Identity with Credential Exchange Protocol Interoperability), integrating DIDComm and OID4VC protocols within a multi-tenancy architecture that enables a single server instance to serve multiple users while maintaining security and data isolation. The system supports critical operations such as authentication, issuance, verification, and credential revocation through protocol abstraction, allowing users to leverage the advantages of each protocol without understanding their technical differences. Testing reveals that OID4VC excels in large-scale credential issuance efficiency as it doesn't require direct connections, while Aries-DIDComm ensures stronger security in verification processes requiring secure connections. Credential formats such as SD-JWT support selective disclosure for enhanced privacy, whereas JWT offers faster verification for simpler use cases. By addressing interoperability challenges and leveraging the strengths of these protocols and formats, this research strengthens the digital identity ecosystem, providing a secure, scalable, and inclusive foundation.

Keywords : Self-Sovereign Identity, interoperability, credential exchange protocols, decentralized identity, Aries-DIDComm, OID4VC