[redacted]

From: dig-comments@list.nist.gov on behalf of Flemming [redacted]
Sent: Tuesday, September 3, 2024 4:41 AM
To: dig-comments@nist.gov
Subject: [dig-comments] Comment on NIST SP 800-63-4 Digital Identity Guidelines: Concordium's Potential Contributions

To Whom It May Concern:

I am writing as a private citizen to provide feedback on the NIST Special Publication 800-63-4, Digital Identity Guidelines. In my research, I have found that Concordium, a public blockchain platform, offers innovative solutions that could significantly enhance the implementation of these guidelines.

1. Privacy-Preserving Identity Proofing and Authentication

Concordium's blockchain technology features an integrated identity layer that allows for the creation of verifiable identities while maintaining user privacy. This is achieved through zero-knowledge proofs (ZKP), which enable users to authenticate themselves without disclosing unnecessary information. This aligns well with NIST's emphasis on strong identity proofing that minimizes privacy risks.

2. Immutable and Transparent Credential Management

Concordium supports the issuance and management of verifiable credentials on its blockchain. These credentials are immutable, meaning they cannot be altered once issued, and are verifiable on-chain. This ensures transparency and security, which are key components of the SP 800-63-4 guidelines.

3. Compliance-Ready Infrastructure

The Concordium blockchain is designed with compliance in mind. It provides a transparent and immutable audit trail, which facilitates adherence to regulatory requirements and aligns with NIST's goals for accountability and security in digital identity systems.

4. Enhanced Security Through Decentralization

By utilizing a decentralized network, Concordium significantly reduces the risk associated with centralized identity systems. This decentralized approach enhances security by eliminating single points of failure, which is critical for the protection of digital identities.

5. Support for Attribute-Based Access Control (ABAC)

Concordium can support attribute-based access control by securely linking user attributes to their identities and ensuring these attributes are verifiable and manageable according to NIST's guidelines. This allows for secure and transparent access control decisions.

6. Interoperability and Scalability

Concordium is built to be interoperable with existing identity management systems and supports various identity protocols. This ensures scalability and flexibility, which are essential for evolving digital identity systems as envisioned by NIST.

Conclusion

Concordium's blockchain technology presents a robust framework that aligns with and can enhance the implementation of NIST's Digital Identity Guidelines. As a private citizen, I believe that incorporating such innovative solutions could greatly improve the security, privacy, and compliance aspects of digital identity systems.

Thank you for considering my comments.

Sincerely,

Flemming Sorensen