



Powering Passwordless through Decentralized Identity


Executive Summary

This white paper explores the significance of decentralized identity (DID) and its role in enabling passwordless authentication. It highlights the importance of self-sovereign identity, emphasizing the need for individuals to have control over their own personal data. The paper also discusses why a decentralized approach is the future of identity management, outlining the benefits it offers in terms of security, privacy, and user experience. Furthermore, it provides a comprehensive overview of DIDs and Verified Credentials as fundamental components of decentralized identity systems.

.

Why a Decentralized Approach is the Future

A decentralized approach to identity management offers numerous advantages over traditional, centralized systems. Firstly, it enhances security by eliminating single points of failure and reducing the risk of data breaches. Decentralization also fosters privacy by minimizing the collection and storage of personal data by third parties. Moreover, it promotes interoperability and portability, enabling seamless identity verification across multiple platforms and services. Lastly, a decentralized approach empowers users, allowing them to manage and control their identities, resulting in increased user trust and satisfaction.



The Problem with Passwords, SSH Keys and Vaults

Modern-day password managers, passwords, and SSH keys, while providing convenience and security in managing credentials, are not immune to certain disadvantages and vulnerabilities that can lead to credential hacks. Let's explore some of these limitations:

SINGLE POINT OF FAILURE

Password managers and vaults, despite being encrypted and offering a centralized storage for passwords, can become a single point of failure. If the master password or the encryption mechanism is compromised, it could lead to unauthorized access to all stored credentials. A successful attack on the password manager can expose all passwords, putting multiple accounts at risk simultaneously.

VULNERABILITIES IN PASSWORDS

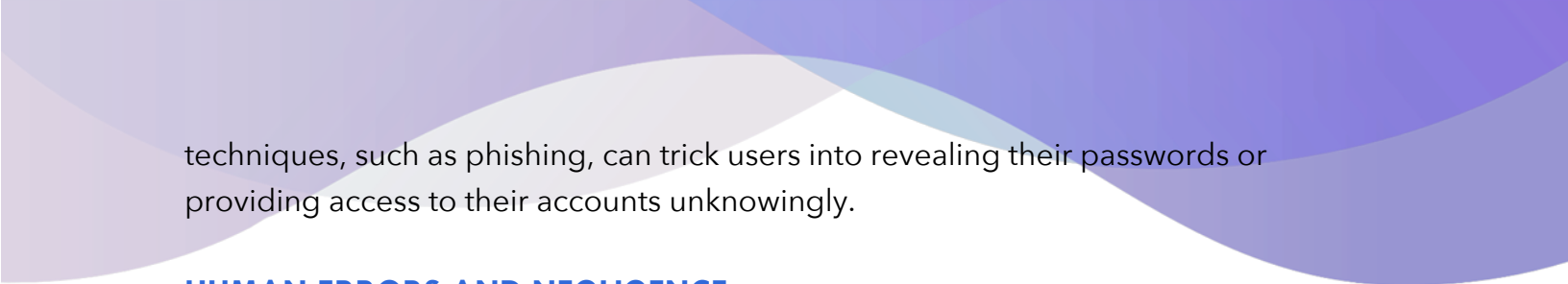
Passwords themselves are susceptible to various vulnerabilities. Weak or easily guessable passwords can be easily cracked using brute-force or dictionary attacks. Additionally, users tend to reuse passwords across multiple accounts, which amplifies the impact of a single compromised password. Moreover, users may unknowingly fall prey to phishing attacks or inadvertently disclose their passwords, further exposing their accounts.

SSH KEY MANAGEMENT

SSH (Secure Shell) keys are widely used for secure remote access to servers and systems. However, improper SSH key management can introduce risks. If SSH keys are not generated with sufficient randomness or are not protected by passphrases, they can be compromised. Additionally, managing a large number of SSH keys across various systems and users can become challenging and prone to misconfigurations or unauthorized access.

INSIDER THREATS AND SOCIAL ENGINEERING

Credential hacks are not limited to external attackers; insider threats and social engineering also pose risks. Malicious insiders or individuals with access to sensitive systems can abuse their privileges to steal or misuse credentials. Social engineering



techniques, such as phishing, can trick users into revealing their passwords or providing access to their accounts unknowingly.

HUMAN ERRORS AND NEGLIGENCE

Human errors and negligence play a significant role in credential hacks. Users may inadvertently share passwords, write them down insecurely, or choose weak passwords. Additionally, negligence in implementing proper security practices, such as not updating software or failing to revoke access for inactive accounts, can leave systems and credentials vulnerable to attacks.

CREDENTIAL STUFFING AND BRUTE-FORCE ATTACKS


Credential stuffing is a prevalent attack where attackers use automated tools to try stolen username and password combinations across multiple websites or services. Since many users tend to reuse passwords, successful credential stuffing attacks can lead to unauthorized access to multiple accounts. Brute-force attacks, which systematically guess passwords, can also be used to crack weak or poorly protected credentials.

THIRD-PARTY VULNERABILITIES

Password managers, SSH key management tools, and even the infrastructure supporting these systems can have vulnerabilities. These vulnerabilities could be due to software bugs, insecure storage practices, or weaknesses in encryption algorithms. Exploiting such vulnerabilities can provide attackers with unauthorized access to the stored credentials.

Self Sovereign Identity

Self-sovereign identity (SSI) refers to an individual's ability to have full ownership, control, and agency over their digital identity and personal data. It empowers individuals with the authority to manage their identities independent of any centralized authority or third-party intermediaries. SSI is built on principles of privacy, security, and user-centric control, aiming to address the limitations and risks associated with traditional identity systems.





OWNERSHIP AND CONTROL

Self-sovereign identity emphasizes that individuals should have complete ownership and control over their personal data. In traditional identity systems, personal data is often stored and controlled by centralized organizations, leading to concerns about data misuse, unauthorized access, and lack of transparency. SSI enables individuals to securely manage their identity-related information, granting them the ability to choose when, where, and with whom they share their data.

PRIVACY AND SECURITY

SSI promotes privacy by minimizing the collection and storage of personal data by intermediaries. It allows individuals to share only the necessary attributes or claims required for a particular interaction, without revealing additional sensitive information. Decentralized technologies, such as distributed ledgers or blockchain, can be leveraged to ensure the integrity and immutability of identity-related data, reducing the risk of data breaches and identity theft.

USER-CENTRIC CONTROL

Centralized identity systems often lack user-centricity, as individuals have limited control over how their personal information is used and shared. SSI puts individuals at the center of the identity ecosystem, enabling them to manage their identities according to their preferences and needs. Users can choose the level of granularity in sharing their data, maintain a comprehensive record of their interactions, and easily revoke or update permissions granted to third parties.

INTEROPERABILITY AND PORTABILITY

SSI enables interoperability and portability of identities across different platforms, services, and domains. With traditional systems, individuals often need to create and manage multiple identities, usernames, and passwords for various online services. SSI provides a unified and portable identity that can be seamlessly verified and trusted across different contexts, reducing the burden of managing numerous credentials.

TRUST AND TRANSPARENCY

In SSI, trust is established through verifiable credentials and cryptographic proofs. Identity claims are issued by trusted issuers and can be cryptographically verified, providing a high level of assurance without revealing unnecessary personal details. This transparent and auditable approach builds trust between individuals, organizations, and service providers, fostering secure interactions in digital environments.

EMPOWERMENT AND INCLUSION

SSI has the potential to empower individuals who may lack traditional forms of identification, such as refugees, marginalized communities, or individuals without official documents. By providing individuals with a self-sovereign identity, they gain access to services, participate in the digital economy, and exercise their rights and privileges. SSI promotes inclusivity, ensuring that everyone can assert their identities and engage in digital interactions on equal terms.

In conclusion, self-sovereign identity is crucial in transforming the way we manage and control our digital identities. It empowers individuals with ownership, privacy, and control over their personal data, enhances security, fosters trust, and promotes interoperability. By embracing SSI principles and leveraging decentralized technologies, we can build a more user-centric, privacy-preserving, and inclusive digital identity ecosystem.

The Approach to Decentralized Identity - A Systems Design Guide

Designing a decentralized identity system involves various considerations. Key elements include:

DECENTRALIZED IDENTIFIERS (DIDS)

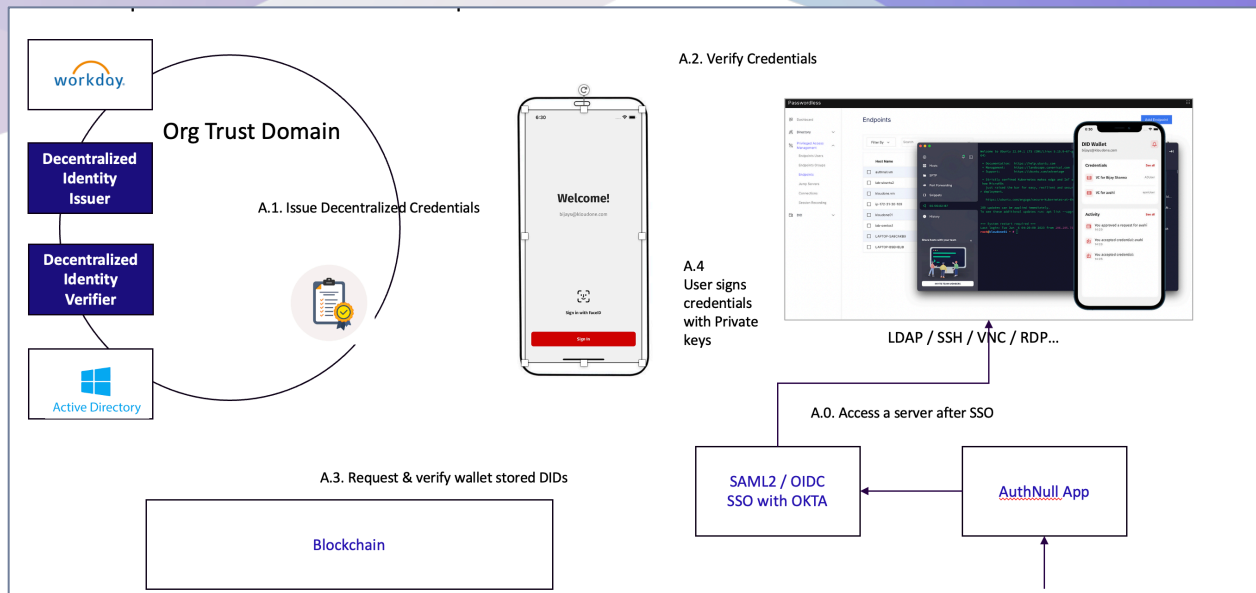
DIDs are the foundation of decentralized identity systems. They are unique, globally resolvable identifiers that allow individuals to assert control over their identities. DIDs are portable, cryptographically secure, and blockchain agnostic. They enable individuals to create and manage their digital identities independent of any specific organization or platform.

VERIFIED CREDENTIALS

Verified Credentials enable the issuance and presentation of digitally verifiable claims about an individual's attributes, qualifications, or achievements. They provide a secure and privacy-preserving method of sharing personal information, allowing individuals to present their credentials without revealing unnecessary details. Verified Credentials enhance trust and simplify the authentication process, laying the groundwork for passwordless authentication mechanisms

A typical system consists of

1. Organization as the issuer of identities, credentials
2. User as the holder of credentials using a decentralized wallet
3. Verifier also owned by the organization which verifies credentials



The organization verifies a users identity and issues credentials.

The user attempts to login to critical infrastructure and is prompted to verify credentials on wallet. Once the user presents the credentials, and the organization verifies it (signed with the users's private keys) the user is able to login to the desired system.

Passwordless Authentication Enabled by Decentralized Identity

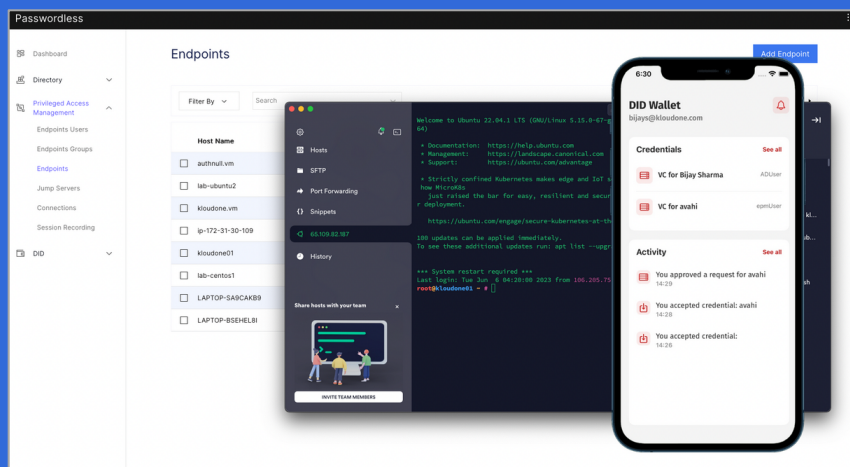
Decentralized identity systems inherently facilitate passwordless authentication. By leveraging DIDs and Verified Credentials, users can authenticate themselves securely and conveniently without relying on traditional username-password combinations. Passwordless authentication methods include biometric authentication, hardware tokens, cryptographic proofs, and multi-factor authentication. These mechanisms enhance security while improving user experience by eliminating the need to remember and manage passwords.

AuthNull's Passwordless Platform

AuthNull enables simplified Passwordless platform for accessing critical infrastructure without using passwords, or SSH Keys.

AuthNull

- Eliminates SSH Keys and Passwords, rotation and distribution and introduce Passwordless 1FA.
- Support for Passwords / SSH Keys with Passwordless 2FA where backward compatibility is required
- Removes the need for a Centralized Vault, a major attack vector.



AuthNull provides a full blown Privileged Access Management (PAM) solution that includes session recording, jump server, endpoint management, vault-less credential management and more.

Learn more at <https://authnull.com>