ANONYOME LABS

Decentralized Identity for Dummies

AKA: Demystifying DI

Decentralized Identity (DI) is an approach to identify and authenticate users and entities without a centralized authority. In traditional identity management and authentication approaches an organization must act as the authority for storing, verifying the validity and reputability of the identity or credentials associated with it, and managing the lifecycle of the identity and its permissions.

Decentralized Identity overcomes the limitations of traditional models – such as federation – by:

- **Relieving the organization of the administrative burden of being a centralized authority.**
- **Placing the user in control of their data.**
- **Removing the overhead of dedicated and disjointed authentication and authorization systems.**
- **Eliminating the need for organizations to gather, store, distribute, and verify personally identifiable information of its customers and/or users.**

Benefits of Decentralized Identity

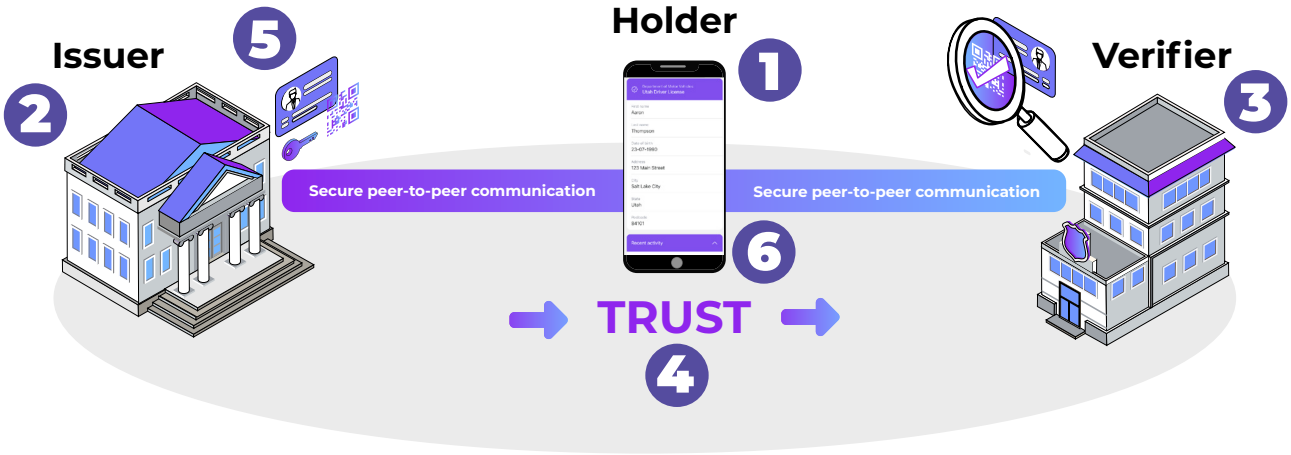
- Streamline processes
- Reduce risk
- Remove the need for manual intervention
- Improve customer / user experiences and safety
- Accelerate sign-up and sign-on
- Facilitate easier compliance

How does DI work?

In a DI scenario:

1. Users hold their own credentials – also called decentralized identifiers (DID) – in an identity wallet.
2. These credentials are provided by organizations that traditionally provide this type of verified information – for examples governments for drivers licenses and passports, credit bureaus for credit scores, regulatory bodies for proof-of-compliance, identity management systems for authorization information, and much more.
3. The user presents their verifiable credentials to the party (called the verifier) that will use the DID to validate identity, qualification, or other required information.
4. The validity of the verifiable credential is attested based on a previously agreed upon trust model and requires no storage of the user's information at the verifier.
5. Upon acceptance of the user-provided credentials, the verifier grants access, approves certification, attests to qualification, or any number of other transactions that previously placed a high storage, risk, and attestation burden on organizations.
6. The entire ecosystem is end-to-end encrypted assuring maximum security and privacy and creating a dedicated, secure, and irrefutable communication channel.

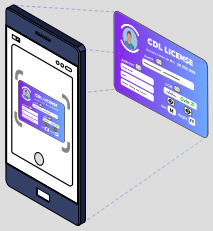
It looks like this:



Where can DI help?

Decentralized identity improves any use case it's applied to. For example:

Compliance – Streamline the "trusted data" processes required for regulatory compliance such as consortium-based data exchange and verification in the agriculture, mining, and energy industries and government-mandated compliance such as GDPR and CCPA.

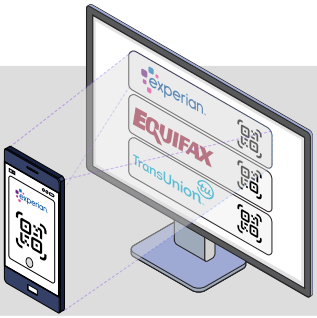


Proof of Qualification – Give individuals who must prove their proficiency and certification to work in certain industries -- such as transportation and construction – complete control over their own credentials

Identity and Access Management – Enforce each user's correct level of access and entitlements to physical or digital resources via very granular permissions including the ability to eliminate password-based logins.

Travel Verification – Remove the burden for multiple, disjointed credentials such as passport, visas, and vaccination status required for travel.

Healthcare Record Privacy – Preserve privacy and secure access around medical history, vaccination status, allergies, preexisting conditions, medications, religious considerations, and other sensitive information.

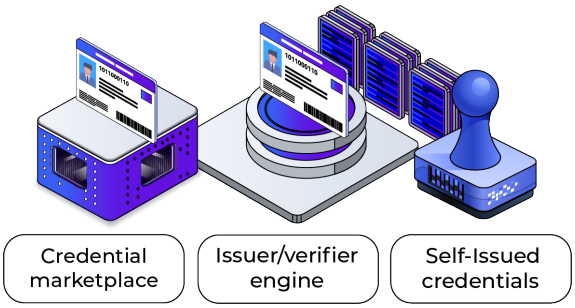


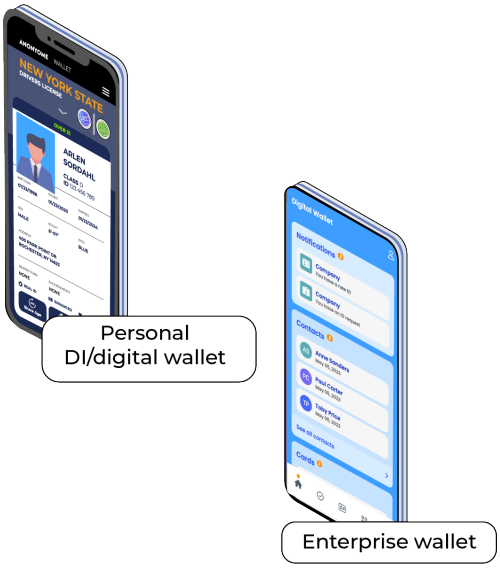
And more – Any use case with verification-heavy requirements, friction in sign-up and sign-in, and silos of permissions, data and identity provider duplication, security risk, and cumbersome end user experiences can benefit from a move to DI.

Making DI real

In order to implement a DI ecosystem a number of components are required, including:

Verifiable Credential Services – Provide the ability to issue and verify digital credentials without the need for a third party or centralized authority. More secure than centralized database models, verifiable credentials leverage decentralized identity technology to extend trust and preserve privacy.

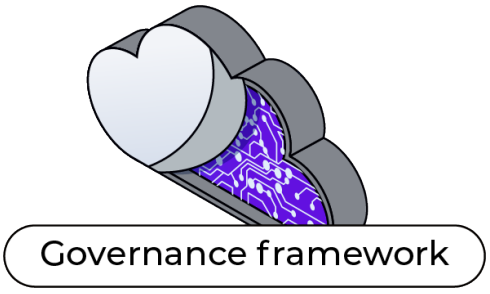




Personal DI Wallet – Equip users to store decentralized identifiers (DIDs), cryptographic keys, verifiable credentials, connections, and other artifacts so they can participate in DI-based actions such as establishing peer-to-peer connections with other users and services; receiving, holding, presenting, and managing data within verifiable credentials; using encrypted messaging, and more.

Enterprise DI Wallet – Acts as the command-and-control center for DI-based activities to easily issue, store, manage, verify and present verifiable credentials.

DI Governance Manager – Empower DI participants to enforce rules while staying true to the tenants of decentralized identity. Organizations can define and enforce governance rules associated with their ecosystem including which wallets, issuers, verifiers are trusted and which credentials are allowed to be used and requested.



Building any (let alone all) of these component of a viable DI implementation is typically beyond the abilities, and budgets of the organizations that would benefit the most from DI. However there is quick, easy, and thorough path to realizing the benefits of DI. Through Anonyme Labs' Sudo Platform, we've done the hard work so you can reap the benefits.

Sudo Platform includes everything you need to quickly bring new DI-based products and services to market or augment existing deployments. It includes: developer-focused documentation, APIs, SDK source code via GitHub, sample applications for test-to-deploy of various capabilities, and brandable apps for quick go-to-market and enterprise deployments. With Sudo platform you can seamlessly add any, or all, of the necessary components of DI in a fraction of the time and at a much lower cost than you may expect.