**Success Criteria**

The core spirits of web3 are decentralization and data autonomy, which can make the implementation of traditional KYC processes challenging, as they often require the collection and storage of personal data, which goes against the core principles of web3. However, ZKPs-based KYC offers a solution to this challenge, providing a way to verify users' identities while still maintaining data autonomy and decentralization.

Here are some of the key business requirements for implementing ZKPs-based KYC in the web3 ecosystem:

* **Privacy**: With ZKPs-based KYC, businesses can verify users' identities without requiring them to disclose their personal information. This can help to protect users' privacy, as their data is not stored on a centralized server or shared with third parties.
* **Regulatory Compliance**: Many businesses operating in the web3 ecosystem are subject to regulatory requirements, such as anti-money laundering (AML) and know-your-customer (KYC) regulations, incl. Identity recovery capabilities for at least five years after the completion of a service relationship given reasonable suspicion and regulatory intervention, and the need for travel rule of KYC data among financial institutions. ZKPs-based KYC can help businesses comply with these regulations while still maintaining the decentralized and autonomous nature of the web3 ecosystem.
* **Security**: By implementing ZKPs-based KYC, businesses can enhance security and reduce the risk of fraud, identity theft, and other malicious activities. The use of ZKPs allows for secure identity verification without the need for centralized identity repositories, which can be a target for attackers.
* **Efficiency**: Traditional KYC processes can be time-consuming and expensive, which can create a barrier to entry for some businesses. ZKPs-based KYC can improve efficiency by reducing the time and cost associated with verifying user identities.
* **User Experience**: With ZKPs-based KYC, users can enjoy a more seamless and user-friendly experience when accessing web3 applications and services. The process of identity verification is simplified, reducing the friction that can sometimes exist with traditional KYC processes.

# Why end-to-end zero knowledge?

## Issues with zkKYC using third-party KYC solutions

* **Privacy Issues**: Integrating a third-party KYC solution means sharing users' personal information with a third-party, which could lead to privacy breaches.
* **Data Ownership Issues**: In a third-party KYC solution, users' source files might be owned and controlled by the third-party, which goes against the principle of user data ownership in web3.
* **Decentralization Issues**: If a decentralized application integrates a third-party KYC, then that application becomes a centralized platform, contradicting the principle of decentralization in web3.

## zkMe's zkKYC design philosophy

* **Personal Data Protection**: In a zero-knowledge proof (ZKP) system, users can verify certain attributes about themselves without revealing raw data. This approach protects user privacy, and users have full control over their own data. This aligns perfectly with the web3 philosophy of decentralization and user sovereignty.
* **Regulatory Compliance**: In situations where KYC/AML checks are necessary, zero-knowledge proofs can provide a solution that balances regulatory compliance with privacy. Users can prove they meet KYC/AML requirements without revealing personal information to service providers.
* **Data Recoverability**: As users control their own data in a zero-knowledge system, they can recover and migrate their data if there are issues with the system or service provider.

<https://docs.zk.me/zkme-dochub/zkkyc-compliance-suite/success-criteria>