**zkMe zkKYC**

**What is zkKYC?**

zkKYC is a solution that enables Web3 businesses to comply with regulations while maintaining decentralization and the privacy and security of their customers' data. It uses zero-knowledge proofs to verify user identity without revealing sensitive information, making it possible to fulfill global KYC requirements in the least intrusive way possible.

**Compliance meets decentralization with zkKYC**

zkMe zkKYC enables Web3 businesses to comply with regulations while maintaining decentralization and the privacy and security of your customers' data.

* **Safeguard your reputation**

zkKYC can help crypto projects detect users' potential affiliation with money laundering and other malicious activities.

* **Stay ahead of the new regulations**

Staying ahead of the curve and ensuring that businesses are fully compliant with regulations.

**Why zkMe zkKYC?**

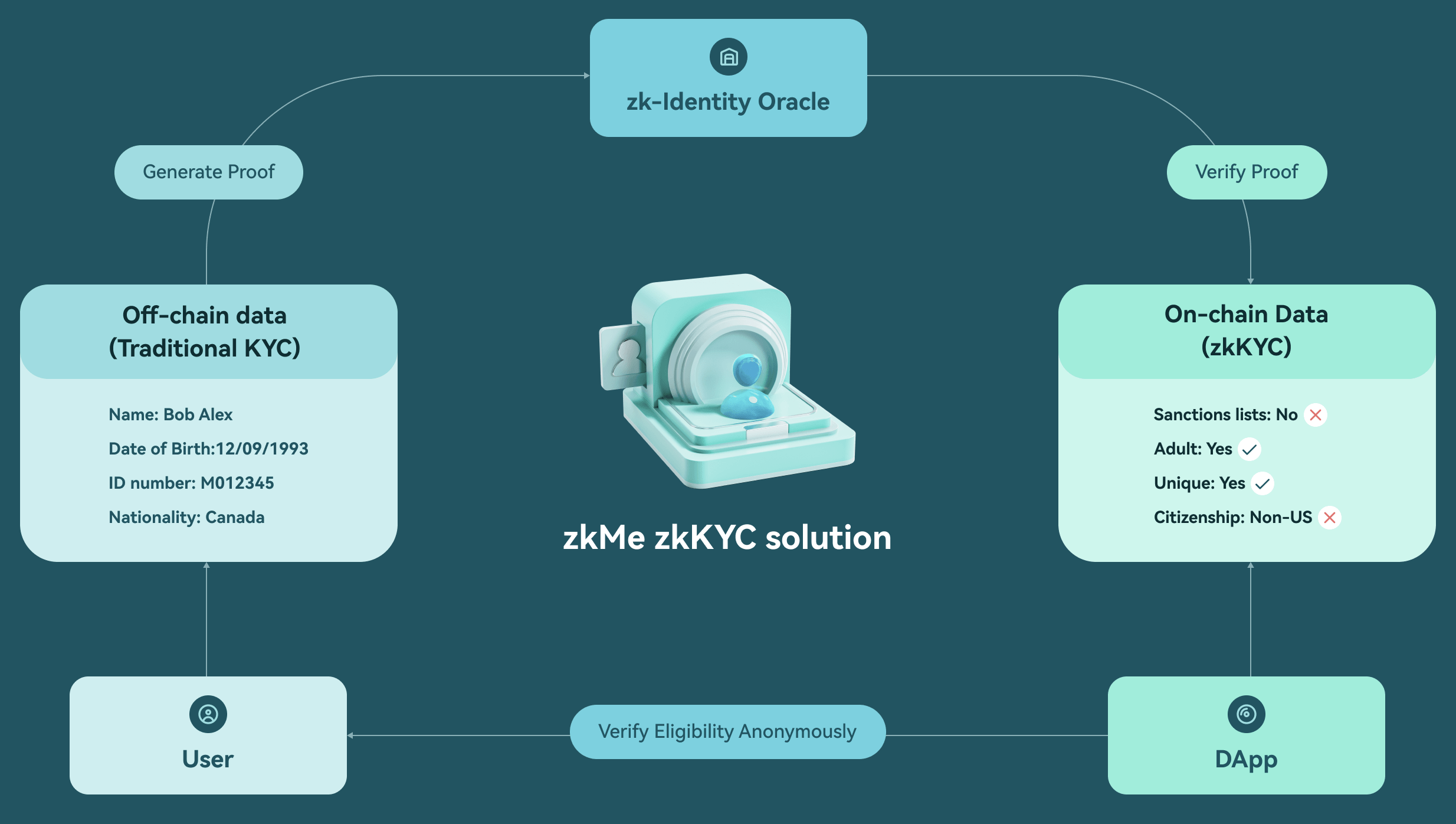
* **Privacy first:** Protect users' privacy with advanced cryptography technologies.
* **Decentralised:** No fixed or controlled role in zkMe zkKYC by a single entity.
* **Fulfil compliance requirement:** Meet global KYC requirements while minimizing intrusion.
* **Reuseable zkKYC:** Users only need to be verified once to access multiple partnered services.
* **Full security:** No personally identifiable information is stored in a central server, eliminating the risk of data leaks.
* **Seamless integration:** Easily integrate your entire verification flow within seconds using our Web and Mobile SDK.

**zkMe zkKYC features**

* **Liveness check:** Use biometric live checks to eliminate bots.
* **Face match:** Compare your users to identify duplicates.
* **Identity check:** Identify forged documents quickly and accurately.
* **Background screening:** Avoid contact with individuals who are at high risk for infection.
* **Proof of address:** Verify your user's proof of residency.
* **Ongoing monitoring:** Conduct continuous know your transaction screening.

**How does it work?**

​



**Technology advancements**

* **Fully customisable**

Use zkMe to customize your workflow and integrate your verification process quickly and easily with our web and mobile SDK.

* **Decentralized storage**

Data is stored in IPFS and is encrypted using threshold signature encryption.

* **Threshold signature encryption**

No single party can reveal a user's identity raw files by using one shard of keys.

* **Smart contract verification**

A smart contract is used to determine whether each verified credential meets predetermined qualifications, based on yes or no answers.

* **Zero knowledge proofs**

ZKPs involves converting the user's information into a mathematical equation that can be verified without revealing any of the underlying information.

* **Frictionless process**

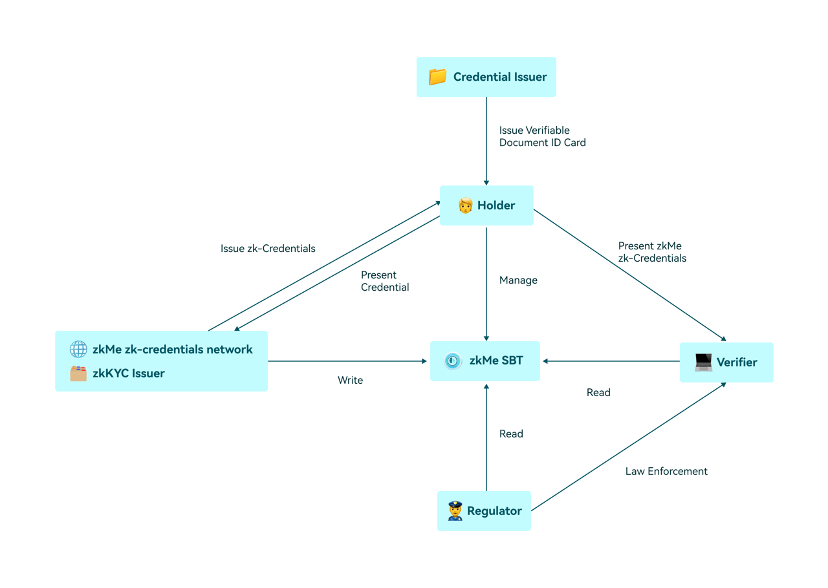
Reduce user friction by easily integrating into websites or mobile apps, allowing users to identify themselves with their preferred device.

**zkMe zkKYC Overview**

zkMe evolves the Roles of SSI verifications and the eKYC process to address aforementioned success criteria.

**The SSI roles evolved**

As an evolution of the roles needed for SSI, zkMe defines Roles with new interactions.



zkMe zkKYC role concept

**Issuer:** In contrast to the traditional SSI role concept, zkMe splits the Issuer role into a trusted Issuer to Issue the verified credentials and the verified presentations.

* Credential Issuer: Refers to governmental or financial entities or organizations that issue physical or digital credentials (such as Passports or ID cards) to individual Holders. This role is equivalent to the role of the Issuer within the traditional SSI concept.
* ZKP Issuer: zkKYC specific concept that refers not to a person or entity, but instead to a trusted Issuer program running directly on the Holder's end device (through the use of Trusted Cryptographic Setups and open-sourced and audited algorithms) uses ZKP technology to process the credentials provided by the Holder and generate VPs in the form of ZKP. zkMe enables eligibility proofs, which are ZKPs that the Holder meets the criteria set out by the Verifier to provide access to the requested service. By leveraging the information in VC, eligibility proofs allow for authentication without disclosing the actual information itself to anyone. For example, a proof can demonstrate that the Holder is of a certain age, is a domestic resident, not on a sanctions list, or not a politically exposed person. This innovative approach to identity verification not only improves privacy and security, but also increases efficiency and convenience for businesses and users alike.

The security of a cryptographic protocol is of paramount importance, especially in the case of zkMe network which is based on zero-knowledge proofs (ZKPs). A robust security model is essential to ensure the protocol's resistance against potential attacks. This chapter presents the ideal functionality for zkMe along with its security goals and security proofs.

**Holder:** This role remains mostly unchanged to the one proposed in the SSI concept. Refers to individuals that hold VC that can be used for various purposes such as accessing services, proving identity, or providing proof of qualifications or certifications. Holder can use their VC to access various services without the need for repeated identity verification. In zkKYC processes, a Holder can trust that their credentials are proven to a Verifier without disclosing private details.

**Verifier:** Verifiers in zkKYC check the authenticity and correctness of a VP claim without the need for the Holder of the credential to reveal sensitive personal information. The Verifier checks the proof against a set of rules or criteria, such as checking that the proof is cryptographically secure and that it matches the information stored on the blockchain. If the proof is valid, the Verifier can be confident that the information provided by the holder of the credential is accurate without having knowledge of the underlying information itself. The Verifier can check the proof against the set of rules or criteria, such as checking that the user is of legal age or is a resident of a particular jurisdiction, without actually processing the Holder's personal information

**Regulator:** The goal of the regulator role in a zkKYC process remains unchanged; materially, it is, however, given a direct role in keeping the data of the Holder private. As the Regulator holds one of three key shards required to uncover a Holder's identity, none of the stakeholders involved (incl. the regulator itself) can remove the veil of Holder anonymity on their own.

**zkMe SBT:** In zkKYC, the verifiable data registry is replaced with an SBT asset stored on public distributed ledgers, that point towards the decentralized storage that contains the ZKP. In contrast to typical SSI implementations, only anonymized VP claims are stored, claims are explicitly designed to not allow for indirect Holder identification, and are only accessible to authorized stakeholders. The zkMe SBT token revolutionizes the way we handle identity and credentials in the web3 ecosystem. The zkMe SBT is the on-chain representation of a Holder's Identity. It contains their DID, ZKP, and one of three key shards used to encrypt and protect the raw data of the holders.

**The KYC process restructured**

zkMe zkKYC enables users to prove their identity to a service provider without revealing their personal information, improving privacy and security over existing eKYC solutions. The process can also help service providers comply with regulatory requirements for KYC while reducing the risk of data breaches, identity theft and verification costs in general. The restructured process of zkKYC involves the following steps:

**Credential Verification:** The Holder submits their identity documentation digitally to the zkKYC Issuer for verification. This step involves the traditional process of providing personal information and documents, such as a passport or driver's license. The Holder's Identity documentation and likeness is verified through OCR and Facial Recognition checks. The zkKYC Issuer algorithm is able to parse the machine-readable identity documents in a structured way. No need for any human interaction or third-party processing.

**Screening & Risk Assessment:** The Holder Identity is screened against lists of known criminals, terrorists, or politically exposed persons (PEPs), transaction history and other relevant information to identify potential risks. This check is processed in real time, no personal data is stored at any time. On basis of the check the zkKYC Issuer generates a risk profile for the Holder Identity and actively scrubs all private user data from memory.

**ZKP Generation:** Once the zkKYC Issuer has verified the holder's identity, it issues an anonymous VP claim (in form of SBT and ZKPs) for each of the preselected eligibility questions. ZKPs provide a mechanism to express traditional credentials digitally, cryptographically secure, privacy-respecting, and machine-verifiable. SBTs are stored on-chain and ZKPs are stored in decentralized storage.

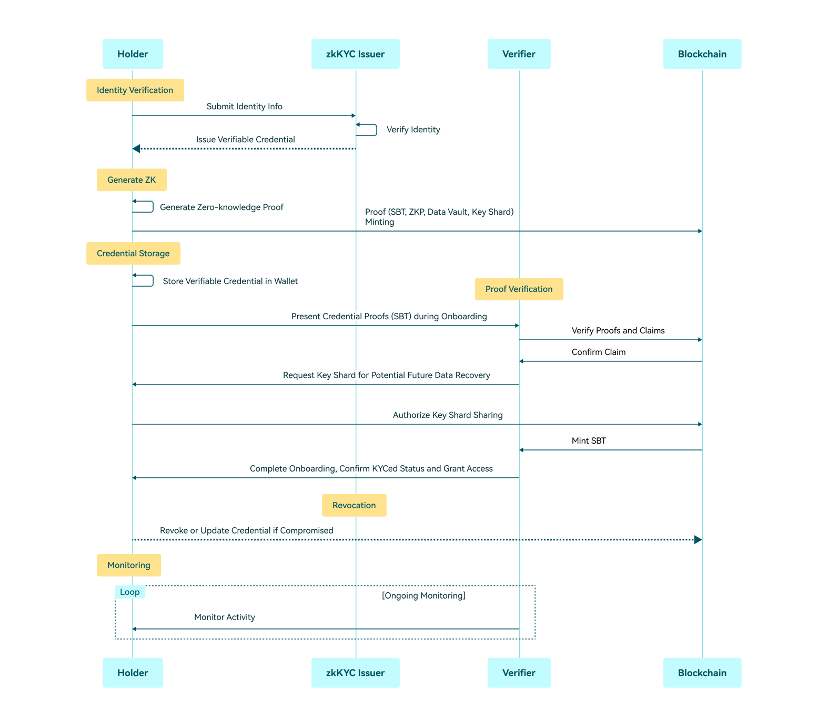
**SBT Mint:** Creation of an encrypted data object to the Holder's SSI wallet that contains their DID and respective ZKP pointers required to prove a Holder’s eligibility to Verifiers repeatedly.

**Proof Verification:** When a Holder wants to access a service that requires KYC, they receive a request to allow for verification of proofs from the Verifier. Once authorized, the Verifier checks the Holder's ZKP against their internal eligibility criteria, such as age or residency. If the proof is valid and the ZKP answers fulfill the service requirements, the user is granted access to the service.

**Proof Revocation:** ZKP VP claims have a natural If the user's verifiable credential is compromised or revoked, the identity issuer can update or revoke the credential, preventing its use for future authentication and verification.

**Ongoing Monitoring:** Verifiers may process continuous on-chain transaction monitoring to ensure compliance with relevant regulations and to detect any suspicious activity that may indicate fraudulent behavior. Additionally, every time a ZKP is reissued upon expiration or revocation, screening and risk assessment procedures are repeated.

**(Data Recovery):** In case, and only in case, the regulator initiates formal bad actor proceedings against a Holder. Upon substantial suspicion, the Regulator, Credential Issuer and Verifier combine their key shards, creating the private key required to unlock the original identity document proof stored in threshold encrypted decentralized storage.



zkMe's zkKYC high level sequence diagram