**What is the zkMe Identity Oracle?**

zkMe is a decentralized web3 credential network that leverages the power of zero-knowledge proofs to enable secure and private credential issuance and verification. With zkMe, users can disclose their credentials to authorized parties selectively, without compromising their privacy, and enjoy greater control over their digital identities.

**As an individual**

You, privately verified.

* zkMe verifies user credentials without disclosing any personal information to anyone (not even zkMe)!
* With zkMe, you can be confident that all your personal information is protected and your interactions with web3 protocols are secure.

**As a web3 protocol**

You can build possibilities based on zk-credentials.

* Eliminate bots and fake accounts instantly with zkProof-of-Personhood anti-sybil protection.
* Avoid jurisdiction by avoiding to onboard users of certain regions with zkGeofencing.
* Comply with regulations by performing zkKYC.
* Verify users' person-bound credential data through open web data attestations and unlock new possibilities.

# Use cases

zkMe's identity oracle enables users to bring their personal data (e.g. credit scores, social network statuses) to the chain. Web3 protocols can then use this data to create tailored features that meet users' needs and preferences. For instance, a DeFi protocol can determine loan eligibility based on credit scores, while a social network can recommend content based on social network status. With zkMe's Identity Oracle, a more personalized and efficient digital world is made possible for each user.

# Mission & Vision

## ****Vision****

To build the zk-credential network of web3. In the trust-less world of tomorrow, credentials are only shared when, where and strictly as irreducibly needed.

## ****Mission****

We build the leading infra for presenting verified credentials in a trust-less and private manner. Issuers, holders and verifiers around the world trust and employ the zkMe protocol to leverage Identities’ value.

An innovative Credential Network protocol that enhances the Self-Sovereign Identity (SSI) model by integrating Verifiable Credentials (VCs), Verifiable Presentations (VPs), Zero-Knowledge Proofs (ZKP), Decentralized Identifiers (DIDs), and Soulbound Token (SBT). Our solution prioritizes **privacy-by-design**, **decentralization**, regulatory **compliance**, and **transparency** to create a comprehensive and secure user experience.

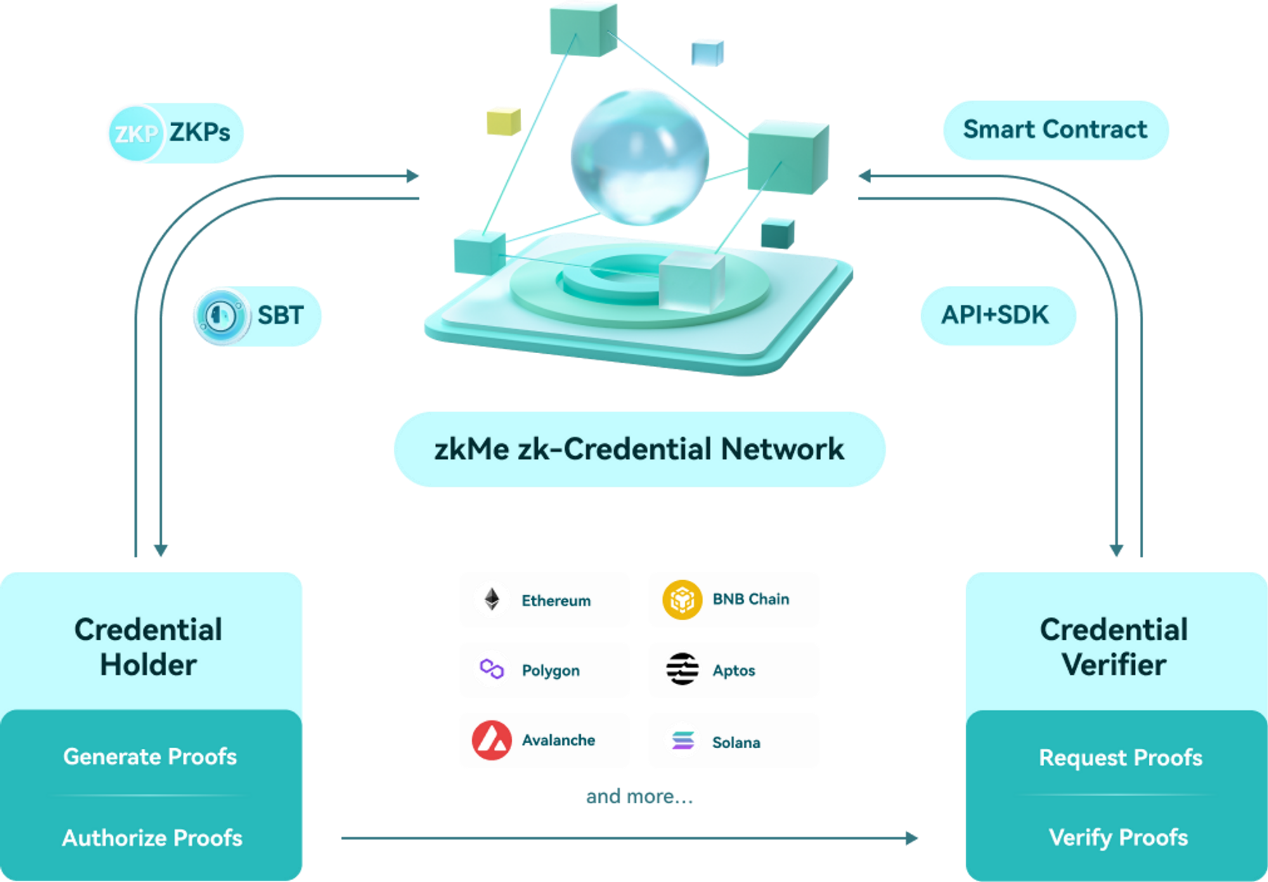
# ****zkMe's Design Philosophy****

zkMe is a comprehensive solution to implement privacy, decentralization, compliance, and transparency in credential networks. Its emphasis end-to-end zero-knowledge processing, and selective information disclosure. Self-Sovereign Identities (SSI) provides users with a high degree of control over their personal data. The platform's compliance with existing and upcoming regulations ensures that it can be used in all industries, ranging finance, to gaming, travel, or even social media.

* zkMe follows a **privacy-by-design** approach above all else in order to guarantee that personal data is processed fully automatically and directly on end devices or within a decentralized oracle network. This ensures that no party can access personally identifying information, and personal data is shared only when absolutely necessary. Users maintain complete control over their information, with the ability to revoke verification permissions on a project-by-project basis via their mobile phones.
* zkMe is committed to **decentralization**. All trust-building determinations and computations are managed by a decentralized network of node operators, minimizing the risk of protocol manipulation and eliminating reliance on proxy verifications. Furthermore, zkMe is party-agnostic, ensuring that no role in the infrastructure is permanently fixed or controlled by a single entity.
* zkMe is designed with regulatory **compliance** in mind, adhering to FATF’s 2019 recommendations for crypto KYC/AML compliance (incl. travel rule requirements), EU’s 6AML and TRF directives, and even upcoming EU MiCA and US Lummis-Gilibrand bill requirements. The platform also complies with W3C DIDs, VC, and VP standards.
* zkMe is both **transparent** and open source. All algorithms necessary for running the infrastructure undergo regular audits and are made available to the ecosystem for the development of additional credential use cases. The platform can process and cross-pollinate credentials across all identity silos, empowering users to benefit from credentials linked to their web3 identities, as well as their real-life or web2 Identities.

zkMe takes the W3C open standard approach of **verifiable credentials** (VCs) and the “Triangle of Trust” (learn more here: <https://en.wikipedia.org/wiki/Verifiable_credentials>), and expands on it by:

* Removing the Issuer trust assumption by replacing the centralized Issuer with **open-source, trustless zero-knowledge verification algorithms.**
* Removing the trust assumption in bridging credentials across (chain-) ecosystems through the use of a **MPC Oracle.**
* Increasing the on-chain availability and reusability of VCs by storing anonymous, zero-knowledge proof presentations (**ZKP VPs**) on-chain in form of non-transferable, non-fungible tokens (**SBT**).
* Decentralizing (and removing the trust assumption) into the Verifiable Data Registry by hosting anonymous proofs on decentralized storage.



# Solution Overview

This chapter presents a high level solution overview of the zkMe network through long-form User Stories for the zkMe Stakeholders, task sequence, and high-level architecture diagram. More details on the single technical components can be found in the following chapter: [Component Overview](https://www.notion.so/Component-Overview-d94e7f85aef94feba3e64fdcc17eca37?pvs=21)

### User Stories

**The Holder** (user)

* The Holder wants to leverage owned off and cross-chain credentials (e.g. a government issued ID card), in order to gain access to permissioned/access controlled services (e.g. permissioned yield pools) on any chain-ecosystem.
* The Holder wants to reveal as little information about him/herself as possible and stay anonymous for as long as possible in order to avoid any party (incl. the Issuer, Verifier or Regulator or any other uninvolved party) to benefit or abuse the link between his/her Identity and public service consumption patterns.
* The Holder values the following metrics (from high to low priority):
  + Low PII Data Sharing Rates
  + Low Average Time to Service (i.e. average time it takes for a user to onboard to a permissioned service)

**The Verifier** (service provider)

* The Verifier needs to fulfill a degree of user due diligence before onboarding a user in order to either
  + fulfill internal business needs (e.g. targeted service provision),
  + reduce fraud (e.g. remove bots & duplicate accounts),
  + avoid jurisdiction (e.g. not provide services to residents of certain countries), or
  + fulfill compliance requirements (e.g. enhanced customer due diligence during onboarding).
* The Verifier requires a solution that is fully decentralized and cost-effective in order to minimize the financial impact of introducing user verification services.
* The Verifier requires a solution that is data minimized and secure from accidental (internal and/or external) user data misuse and leaks in order to fulfills it’s requirements under global data privacy regulations such as EU’s GDPR.
* The Verifier values the following metrics (from high to low priority):
  + High User Verification Retention Rate (i.e. how many users do not drop-off during the verification process)
  + Low Crossover Error Rate (i.e. a combination error of false positive and false negative user verifications)
  + Low Costs per Verification

**The Regulator**

* The Regulator wants to protect Holders (within its legislation) to access unregistered financial services in order to protect the Holder from intransparent risks.
* The Regulator requires the ability to recover the real Identity of a Holder in case formal bad actor proceedings are initiated against the Holder.

### Task Sequence

1. **Initial Verification**

The Holder presents the off-chain credential to an open-sourced verification algorithm that runs locally on the Holder’s end user device (mobile phone). The verification algorithm encodes the results of the verification algorithm through anonymized, tamper-proof ZKPs. The ZKPs are sent to an MPC node Oracle for verification of the proof consistency. Once verified, the MPC node Oracle calls a Mint Smart Contract that mints a credential proof SBT onto the Self-Sovereign Identity Wallet of the Holder.

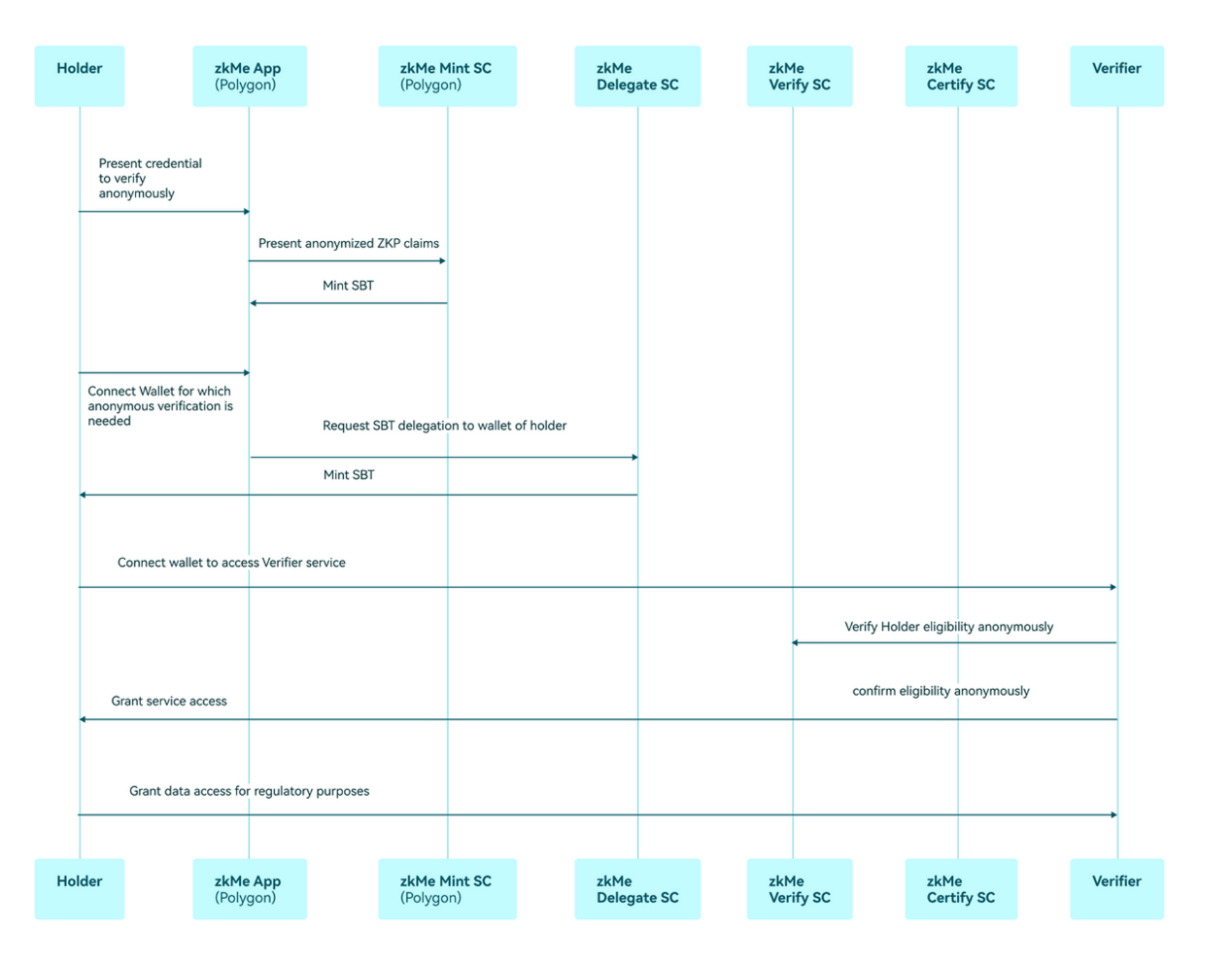
1. **Proof Delegation**

The Holder delegates the credential proof to any chain ecosystem he/she is active in, by signing a delegation transaction from the SSI-Wallet. This calls a Delegate Smart Contract that bridges the SBT onto the chain ecosystem of choice.

1. **Service Onboarding**

The Holder accesses the Service provided by the Verifier by connecting his/her wallet. Depending on the requirement background, the Verifier can either call a Verify or a Certify smart contract to ascertain the eligibility of the Holder. The Verify smart contract allows for a one-time verification (yes/no answer to a ZKP encoded eligibility question) of the Holder credential. The Certify smart contract additionally allows to keep an auditable proof that a verification of the Holder by the Verifier took place and the Regulator may initiate bad actor proceedings against the Holder. Invoking a “certification” requires an additional signature approval by the Holder.

Please note: Tasks 1 through 3 can be processed in one go in case the Holder’s first touchpoint is the Verifier Service and is guided through the verification process using the zkMe Widget.



### Architectural Overview

