# CamuVerify Smart Contract – Phased Verification Model Specification

## Overview

The CamuVerify.sol smart contract governs identity and age verification within the Camuverse ecosystem. To ensure legal compliance and future-proof decentralization, this specification outlines a phased verification model that evolves over time from centralized control to decentralized, cryptographic identity attestations.

## Phased Verification Model

|  |  |  |
| --- | --- | --- |
| Phase | Admin Model | Description |
| Phase 1 | DAO Multisig | Contract ownership is managed by a DAO-controlled multisig wallet. Founders or governance signers act as the verification authority for onboarding users. |
| Phase 2 | Verifier Registry | DAO-controlled registry of trusted KYC or verification providers. Verifiers can be added/removed by governance. Only approved verifiers can call verification functions. |
| Phase 3 | ZKP or DID Integration | Future extensibility to allow verification via decentralized identifiers (DIDs) or zero-knowledge proofs (ZKPs), using protocols like Polygon ID or Verite. Enables self-sovereign, privacy-preserving identity. |

## Key Functions

• verifyMember(address user, uint16 birthYear): Called by admin or approved verifier. Calculates `isAdult`.

• setVerifier(address verifier, bool status): DAO can add/remove verifiers.

• isVerified(address user): Returns true if user has passed verification.

• isAdult(address user): Returns true if user’s birth year qualifies as 18+.

## Compliance & Privacy Considerations

• Personally identifiable information (PII) is never stored on-chain.  
• The contract only retains non-sensitive flags: verification status and adult status.  
• Compatible with Civic, Fractal ID, Veriff, and DID protocols.  
• Upgradable to support off-chain proofs and on-chain attestations.

This phased design ensures that CamuVerify remains lightweight, decentralized, and legally compliant, while giving DAO governance control over verification policy.