Whitepaper [EN]

# zkPass: Building the Verifiable Internet through zkTLS

***Updated: Apr 14 2025***

## ***Table of Contents***

# 1. Executive Summary

For decades, the internet has relied on visibility rather than verifiability.

Data shared across networks can be encrypted but not cryptographically proven to originate from a trusted source without exposing its contents. This structural limitation has made Web2 inherently private but unverifiable, and Web3 verifiable but publicly transparent.

zkPass introduces a new cryptographic primitive — zkTLS (Zero-Knowledge Transport Layer Security) — that transforms any HTTPS session into a verifiable, privacy-preserving proof source.

By combining three-party TLS, multi-party computation (MPC), and interactive zero-knowledge proofs (IZK), zkPass allows users to prove statements about their Web2 data (identity, reputation, assets, learning progress, etc.) without revealing the underlying information.

This architecture establishes zkPass as the verifiability layer of the internet, bridging Web2 trust boundaries and enabling a new generation of decentralized applications powered by authenticated real-world data.

# 2. Background & Motivation

Today's internet is built on TLS, securing over 95 % of all websites through end-to-end encryption.

TLS guarantees confidentiality and integrity but not verifiable authenticity — third parties cannot cryptographically confirm that a piece of data originated from a specific HTTPS domain.

At the same time, the rise of decentralized systems has created a demand for trustless verification of off-chain data.
While Web3 protocols are transparent by design, they lack access to verified Web2 information such as financial records, credentials, and behavioral data, all locked within private servers.

This disconnect produces the Web2–Web3 trust gap:

- Web2 data is private but unverifiable.
- Web3 data is verifiable but public.

zkPass resolves this contradiction. By turning standard TLS sessions into zero-knowledge proofs, zkPass allows users to export private, authenticated Web2 data

into verifiable on-chain proofs — enabling a verifiable internet without compromising privacy.

# 3. zkPass Protocol Architecture

The zkPass protocol redefines the standard TLS communication model by introducing a third cryptographic participant: the Node.

The system involves four logical entities:

| Role | Function |
|---|---|
| Prover (User) | Retrieves private data from Web2 sources and generates a zero-knowledge proof. |
| Verifier (Application) | Validates the proof to confirm statements about user data without learning the data itself. |
| Node (zkPass Network) | Participates in a 3-party handshake to verify authenticity and integrity of the TLS session. |
| Data Source (Server) | The HTTPS endpoint that hosts the original data. |

The resulting design — the 3-Party TLS (3P-TLS) protocol — establishes a privacy-preserving channel between user and server that can be cryptographically verified by a third party.

# 4. Technology Overview

## 4.1. zkTLS

zkTLS extends the traditional two-party TLS into a three-party handshake between the Prover, Node, and Data Source.

The Prover and Node jointly act as the client, while the Data Source acts as the server. Through elliptic-curve Diffie-Hellman key exchange and secure message authentication (MAC) sharing, both parties jointly derive session keys without ever revealing private information.

This design ensures:

- Authenticity — proofs can only be generated from legitimate HTTPS sessions.
- Integrity — data cannot be forged or modified by the user.
- Privacy — neither Node nor Verifier learns any plaintext data.

## 4.2. Multi-Party Computation (MPC)

MPC guarantees that no single party can alter or reconstruct sensitive information.
During proof generation, the Prover and Node each hold partial keys; they must

cooperate to compute message authentication codes, ensuring that only genuine server responses can be attested.
This prevents forgery and enforces cryptographic trust between participants.

### 4. 3. Interactive Zero-Knowledge Proofs (IZK)

Once data integrity is confirmed, zkPass employs VOLE-based IZK to generate proofs directly in browser environments — without a trusted setup.
Users can locally prove statements such as:

- "This account is verified by a licensed exchange."
- "My Duolingo streak exceeds 30 days."
- "My bank account balance is greater than $10 000."

These statements are verifiable on-chain or within decentralized systems, yet reveal nothing about the underlying data values.

### 4. 4. Circuit Factory & Modular Design

zkPass employs modular circuits built on Bristol-style logic (AND/XOR/INV gates).
Each proof circuit corresponds to a "schema," a standardized logical structure for a specific type of verification.
Schemas are reusable, composable, and distributed through the Schema Market, allowing developers to integrate new verification logic without re-engineering the protocol.

## 5. Developer Ecosystem & Use Cases

zkPass provides a full development stack enabling anyone to integrate private verifications into applications:

| Layer | Component | Description |
|---|---|---|
| Protocol Layer | zkTLS | The cryptographic foundation connecting Web2 and Web3. |
| Developer Layer | DevHub | Toolkits, APIs, and SDKs for schema creation and proof generation. |
| Gateway Layer | TransGate SDK | Unified gateway for dApps to verify user proofs with minimal integration effort. |
| Application Layer | Schema Market | A decentralized marketplace for reusable verification schemas. |

Representative Applications

- **Proof of Humanity:** attest verified social, identity, or government credentials.
- **Proof of Learning:** verify academic or skill-based achievements.
- **Proof of Assets:** confirm ownership or balance without exposure.
- **Proof of Participation:** prove event or campaign involvement.
- **Proof of Behavior:** attest off-chain actions (rides, orders, memberships).

As of 2025 Q2, zkPass supports over 100 verified data sources, 300 schemas, and 200 M TVC (Total Verifiable Computation) processed across 80 integration partners.

# 6. Network Economy & Token Model

The internet has always been built on information, but not on verifiable truth. For decades, online data has been visible rather than verifiable. Screenshots can be forged, credentials fabricated, and trust has relied on assumption instead of proof.

zkPass and its zkTLS protocol redefine this foundation. For the first time, private Web2 data such as financial records, identity attestations, learning streaks, or travel histories can be transformed into cryptographic proofs that are portable, privacy-preserving, and verifiable across networks. At the center of this verifiable data economy stands $ZKP, the native utility token that enables settlement, validation, and coordination within the zkPass ecosystem.

## 6.1. Token Overview

- Ticker: $ZKP
- Token Standard: ERC-20
- Total supply: 1,000,000,000
- Supply Type: Fixed, no inflation
- Deflationary Model: Portion of settlement fees burned to keep supply deflationary.
- Buyback Mechanism: DAO-led periodic buybacks funded by protocol revenue.

## 6.2. Token Utility

- **Settlement Medium**: $ZKP is the native functional unit required for proof settlement and verifier execution within the zkPass ecosystem.
- **Validator Collateral**: Validators post $ZKP as operational collateral to ensure network correctness, uptime, and reliability.
- **Network Credits**: $ZKP operates as on-chain credits for recording and accounting network contributions, including verifiable computation and integrations.
- **Service Access**: Used by enterprises and developers to interface with zk-native verification APIs and privacy-preserving data infrastructure.
- **Cross-System Verifiability and Governance**: $ZKP supports decentralized coordination and acts as the trust layer linking verifiable systems, while sustaining audits and other non-profit maintenance activities.6.3 Token Distribution

## 6.3. Token Allocation and Vesting Schedule

- **Community — 48.5%**

*(12.5% unlocked at TGE, 6% vesting linearly over the first 3 months, and 30% vesting monthly over 5 years starting from TGE)*

Allocated for ecosystem growth, including verifiable airdrops, network incentives, community sales, exchange-related marketing, and strategic partnerships.

- **Early Investors — 22.5%**

*(12-month cliff followed by 18-month linear vesting)*
Allocated to strategic and institutional partners who supported early-stage protocol development.

- **Core Contributors — 14%**

*(24-month cliff followed by 24-month linear vesting)*
Reserved for founding members, engineers, researchers, and key operational contributors driving the zkPass network.

- **DAO Treasury — 10%**

*(5-year linear vesting)*
Dedicated to long-term network sustainability, governance, ecosystem grants, and emergency reserves.

- **Liquidity — 5%**

*(100% unlocked at TGE)*
Reserved for market liquidity provision and network bootstrapping.

At launch, circulating supply is limited to community participation and liquidity, with 0% unlocked for the team or investors. Initial Circulating Supply: ≈ 20.167 % at TGE.

### 6.4. The Credibility Flywheel

→ Web2 and Web3 converge, unlocking vast data universes.
→ Data moves through privacy-preserving verification.
→ Verified interactions create real utility and new applications.
→ Utility drives adoption by users and enterprises across ecosystems.
→ Adoption fuels validator participation and network incentives.
→ Growing value accelerates integrations and data onboarding.
→ Each new data source restarts the cycle, faster, stronger, and broader.

Each rotation compounds utility, liquidity, and credibility,
turning trust into energy and energy back into trust.
zkPass is not just building a product.
It is engineering a self-sustaining trust economy for the digital world,
the coordination layer for every system that must prove before it can act.

## 7. Governance & Security Framework

zkPass transitions progressively from a development-led coordination model to full DAO governance.

### 7.1. Governance Layers

zkPass DAO – the ultimate decision-making entity overseeing protocol parameters, treasury, and grant programs.

Core Contributor Committees – non-executive teams (Technology, Ecosystem, Operations, Legal & Compliance, Treasury) executing DAO-approved mandates.

Treasury Multisig Committee – 3-of-5 Safe wallet controlling operational disbursements with DAO oversight.

### 7.2. Voting Rules

Minimum Quorum: 8 % of circulating $ZKP

Standard Proposals: ≥ 50 % majority of votes cast

High-Impact Proposals: ≥ 66 % supermajority for structural changes or treasury reallocations

### 7.3. Security Assumptions

All network nodes perform MPC-verified operations; no single node can forge proofs.

TLS keys are never reconstructed outside browser memory.

Proof verification contracts are deterministic and open-sourced for auditability.

## 8. Roadmap & Outlook

| Phase | Milestone | Description |
|---|---|---|
| Phase I (2022–2023) | Protocol Foundation | zkTLS research and prototype implementation with 3P-TLS, MPC, and IZK integration. |
| Phase II (2024) | Developer Ecosystem | Launch of Schema Market and TransGate SDK; expansion to 80+ integration partners. |
| Phase III (2025) | Decentralized Node Network | zkPass Node Network mainnet launch; proof-weighted staking economy activation. |
| Phase IV (2026+) | Governance & Enterprise Expansion | Full DAO governance; zkTLS enterprise suite for institutional data attestation; multi-chain zkTLS compatibility. |

Strategic Vision:

zkPass envisions an internet where verifiable truth coexists with privacy.

By anchoring Web2 authentication in zero-knowledge cryptography, zkPass transforms private data into public verifiability — establishing the foundation for decentralized identity, verifiable reputation, and privacy-preserving on-chain intelligence.

# 9. Legal & Compliance Statement

zkPass Foundation operates as a non-profit association organized under Swiss civil law, following the governance and transparency requirements applicable to technology-oriented foundations. The Foundation's mandate is to support the open development and maintenance of the zkPass protocol, zkTLS technology, and related infrastructure.

The $ZKP token is designed strictly as a functional utility token within the zkPass ecosystem. It serves as a medium for proof settlement, validator staking, computation metering, and decentralized governance.

$ZKP does not represent equity, ownership, profit-sharing rights, or any claim on future revenue of the Foundation or its contributors.

No holder of $ZKP is entitled to dividends, voting rights in any legal entity, or any guaranteed appreciation of value. All usage is governed by the protocol's on-chain logic and DAO governance procedures.

The zkPass Foundation and its affiliates adhere to international AML/CFT standards and implement compliance measures in token distribution and exchange integrations.

Token sales, if conducted, are limited to eligible jurisdictions in accordance with applicable digital asset and securities regulations. The Foundation will continue to engage licensed counsel in Switzerland, Singapore, and South Korea to ensure that $ZKP maintains its classification as a non-security utility token under relevant legal frameworks.

# 10. Team & History

The development of zkPass has progressed through several distinct phases, each marking a step toward realizing a verifiable and privacy-preserving internet.

The project was founded in Q2 2022 by a team of engineers from NTT Docomo, Tencent, and IBM, combining deep expertise in applied cryptography, network security, and distributed systems. During late 2022, the team completed the early research and implementation of the zkTLS prototype — a first-of-its-kind integration of three-party TLS (3P-TLS), multi-party computation (MPC), and interactive zero-knowledge proofs (IZK).

Throughout 2023, zkPass entered its protocol alpha phase, launching a developer testnet and validating the first ecosystem integrations with external applications. This stage confirmed the feasibility of using TLS-based cryptographic attestations for real-world data verification.

In 2024, the project transitioned from a research initiative into a growing ecosystem. The launch of the Schema Marketand TransGate SDK enabled developers to create and deploy reusable verification schemas across a broad range of use cases. By the end of the

year, zkPass had supported more than 80 integration partners and over 300 schema templates.

By mid-2025, the network reached over 200 million TVC (Total Verifiable Computation) and finalized the validator incentive design together with the initial DAO governance framework — setting the foundation for decentralized node participation.

Looking ahead to 2026 and beyond, zkPass will complete the transition toward full DAO governance and enterprise-grade adoption. The upcoming zkTLS Enterprise Suite will extend verifiable data infrastructure to institutional and cross-chain environments, solidifying zkPass as the foundational verification layer for the internet.

zkPass is developed by a globally distributed team of cryptography researchers, protocol engineers, and Web3 infrastructure experts operating under the zkPass Ecosystem.

Core contributors have backgrounds in large-scale system security, zero-knowledge proof research, and enterprise authentication protocols.

The team coordinates community-driven development, open-source contributions, and technical documentation under the MIT license model.

# 11. Security Audits & Risk Management

Security, privacy, and verifiability are the foundation of the zkPass protocol. To ensure long-term resilience and integrity, zkPass maintains a multi-layer security framework combining formal cryptographic verification, smart contract audits, and operational risk controls.

## 11.1. Protocol-Level Security

- The zkTLS protocol is based on formally verified primitives of MPC and IZK.
- Session keys and MAC shares are generated using threshold cryptography, preventing any single participant from reconstructing plaintext data.
- TLS handshake proofs are verifiable end-to-end, ensuring authenticity and non-repudiation of data origin.
- A comprehensive **security audit report** covering all on-chain contracts and zkTLS protocol modules will be made publicly available upon completion at https://www.halborn.com/audits/zkpass/zkpass---chromium-browser-extension-pentest-220f58

## 11.2. Smart Contract & Network Audits

- All on-chain smart contracts and validator modules will undergo independent audits by industry-recognized security firms (e.g., SlowMist, PeckShield, or Trail of Bits).
- zkPass maintains an internal testing environment for protocol updates, following continuous integration and formal verification procedures before deployment.

- The network will operate an ongoing bug bounty program encouraging responsible vulnerability disclosures and open security collaboration.

## 11.3. Operational Security

- The DAO Treasury and multisig wallets adopt multi-signature (3-of-5) control with periodic rotation of signers.
- Validator registration requires staking of $ZKP and compliance with uptime and reliability metrics.
- Keys and credentials used for node operations are stored using HSM-backed infrastructure, with disaster recovery protocols audited quarterly.

## 11.4. Risk Disclosure

While the zkPass protocol has undergone extensive internal testing, all distributed cryptographic systems carry residual risks related to software bugs, network latency, or third-party dependencies.

The Foundation commits to public transparency in disclosing vulnerabilities and implementing community-driven remediation when necessary.