Tiered Privacy

Restoring Trust in the Digital Age

A Decentralized Framework for Identity and Authenticity Online

Michael Deeb, Keeplist.io & TealWolf Consulting

Co-Founder of Keeplist.io
Director of Civic Tech DC
15 years of engineering experience
6 years in the ML space

The Internet's Trust Problem

The urgent need for trust in an inauthentic world:

- Nearly **50%** of internet traffic comes from automated sources
- **30%** of this traffic is malicious (Imperva, 2024)
- The line between real and fake is increasingly blurring
- Algorithmic manipulation and narrative amplification is rampant
- "Blue checkmarks" and other verification systems often mislead rather than inform

Reclaiming Authentic Anonymity

- The early internet was built on anonymity with assumed authenticity
- Today's online interactions require cryptographic proof of authenticity
- Privacy and trust are not mutually exclusive
- We need a user-centric approach that balances privacy, trust, and usability

> *"We need to cryptographically prove authenticity without sacrificing privacy, while balancing usability and accessibility for widespread adoption."*

Current Solutions Fall Short

Centralized identity systems:

- Privacy risks and surveillance potential
- Single points of failure
- Data breaches and identity theft
- Users forced to share all or no data

Biometric approaches (e.g., Worldcoin):

- Hardware limitations create access barriers
- Ethical concerns around biometric data
- Regulatory pushback globally
- Centralized control of sensitive data

Worldcoin: A Cautionary Tale

- Centralized biometric identity platform requiring iris scans
- For-profit entity controlling all verification hardware and data
- Creates single point of failure and risk of abuse
- Led to regulatory investigations and halts in multiple countries
- Directly contradicts principles of decentralization and data minimization

Introducing TPIF

Tiered **P**rivacy and **I**dentity **F**ramework

- A spectrum of verification options, not a binary system
- User control over personal data disclosure
- Strong cryptographic foundations
- Decentralized, consortium-governed structure
- Universal Proof-of-Personhood as a foundation

Core Principles

1. **Preserve Online Freedom**
    - Keep the internet accessible, decentralized, and equitable
2. **Build Trust Without Compromise**
    - Use cryptography to verify authenticity without revealing data
3. **Raise the Cost of Abuse**
    - Make automated manipulation difficult and expensive
4. **Support Context-Specific Verification**
    - Flexible tiers for different situations and preferences
5. **Enable Secure Anonymous Communication**
    - Protection in politically compromised environments

The 5 Tiers of Privacy

A flexible framework that adapts to different contexts and user needs, governed by community consensus

Tier 1: Anonymous but Authentic

- Complete anonymity with proof of humanity
- Free and universal foundation
- Zero personal information shared
- "Digital birthright" for all users

Applications:

- Whistleblowing and reporting corruption
- Political speech in sensitive contexts
- Communication under oppressive regimes
- Research on sensitive topics

Tier 2: Anonymous but Unique

- Session-based uniqueness for specific interactions
- Prevents multiple accounts/votes without tracking
- Verify credential validity without revealing content
- Like a "fairground token" that proves entry without identifying you

Applications:

- "One person, one vote" systems
- Limited-time offers without persistent accounts
- Anonymous contests and giveaways
- Temporary access systems

Tier 3: Pseudonymous Presence

- Persistent identity within a specific context
- Build reputation and history over time
- No link to real-world identity
- Consistent across sessions on a platform

Applications:

- Online marketplaces (buyer/seller reputation)
- Community forums and discussion boards
- Subscription services
- Persistent platform-specific identities

Tier 4: Moderated Identity

- Third-party verification of specific credentials
- Selective disclosure of verified attributes
- Control over what information is shared with whom
- Link to real-world credentials without full exposure

Applications:

- Professional license verification (doctors, lawyers)
- Proving ownership of assets without full identification
- Controlled access to regulated services
- Privacy-preserving KYC/AML compliance

Tier 5: Public Identity

- Full transparency and accountability
- Real-world identity linked to online presence
- Maximum public trust and verification
- For public-facing roles and official communications

Applications:

- Public figure verification
- Government and official accounts
- High-security contexts
- Public trust roles

TPIF's Core Components

How does TPIF achieve this tiered privacy? Through these key components:

- **Decentralized Identifiers (DIDs):** Tiered spectrum of association with real identity
- **Verifiable Credentials (VCs):** Tamper-proof credentials from trusted issuers
- **Self-Sovereign Identity (SSI):** User ownership and control of digital identity
- **Universal Proof-of-Personhood:** PoP verification required across all tiers
- **Permissioned Blockchain:** Consortium-governed infrastructure
- **FHE-Protected Audit Logs:** Privacy-preserving verification records

Advanced Cryptographic Technologies

Zero-Knowledge Proofs (ZKPs):

- Prove facts without revealing data
- Example: Proving you're over 21 without revealing birthdate

Secure Multi-Party Computation (MPC):

- Verification Oracles collaborate without seeing complete data

Fully Homomorphic Encryption (FHE):

- Compute on encrypted data, enabling "eventual privacy"

Onion Routing (Mix Network):

- Network-level anonymity for all communications

System Architecture

Key flow:

1. User initiates login with TPIF
2. Verification oracles selected
3. Credentials verified via ZKPs
4. Results returned without exposing user data

Privacy-Preserving Login Protocol

1. User initiates login with "Login with TPIF"
2. Client generates a random SessionID
3. Communication routed through Mix Network (onion encryption)
4. Smart contract randomly selects Verification Oracles
5. Client generates ZKPs for required credentials
6. Oracles verify credentials via MPC without seeing data
7. Verification result sent to Relying Party
8. FHE-protected audit logs maintain accountability

Benefits

For Users:

- Reclaim control over personal data
- Granular control over identity disclosure
- Reduced risk of identity theft
- Safer participation for marginalized groups

For Platforms:

- Combat fake accounts and bots
- Higher quality content and interactions
- More effective moderation
- Enhanced user trust

Benefits (continued)

For Organizations:

- Reduce KYC/AML compliance costs
- Reduced data breach liability
- Regulatory compliance with privacy laws
- Secure cross-border data sharing

For Society:

- More trustworthy online environments
- Reduced impact of bots and disinformation
- Protection for vulnerable populations
- Foundation for digital governance

Call to Action

> *"The early internet was built on anonymity and assumed authenticity. We can reclaim that promise with cryptographic proof instead of blind trust."*

- **Join the development community** on GitHub
- Contribute to technical specifications
- Help shape governance structures
- Participate in early adoption and testing
- Spread awareness of privacy-focused identity solutions

Thank You

GitHub: github.com/keeplist-io/keeplist-TPIF

Contact: deeb@keeplist.io

Questions?