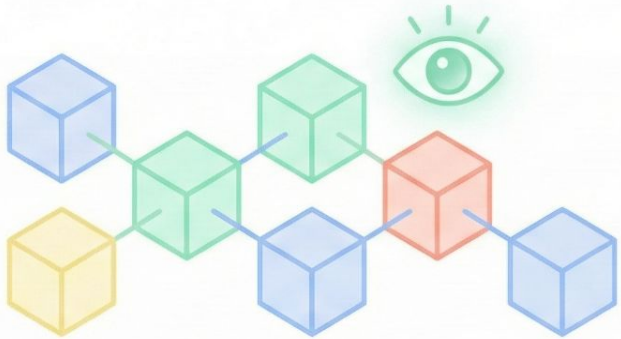
Introducing the did:cel Method

A High-Availability, Censorship-Resistant, Witness-Based DID Method utilizing Cryptographic Event Logs.



High-Availability

Censorship-Resistant

Cryptographic Event Logs

Why did:cel? Design Goals & Philosophy

High decentralization without blockchains or expensive consensus.

Censorship Resistance

No central registry to block identifiers.

Self-Certifying

DID derived directly from initial log state.

Minimal Infrastructure

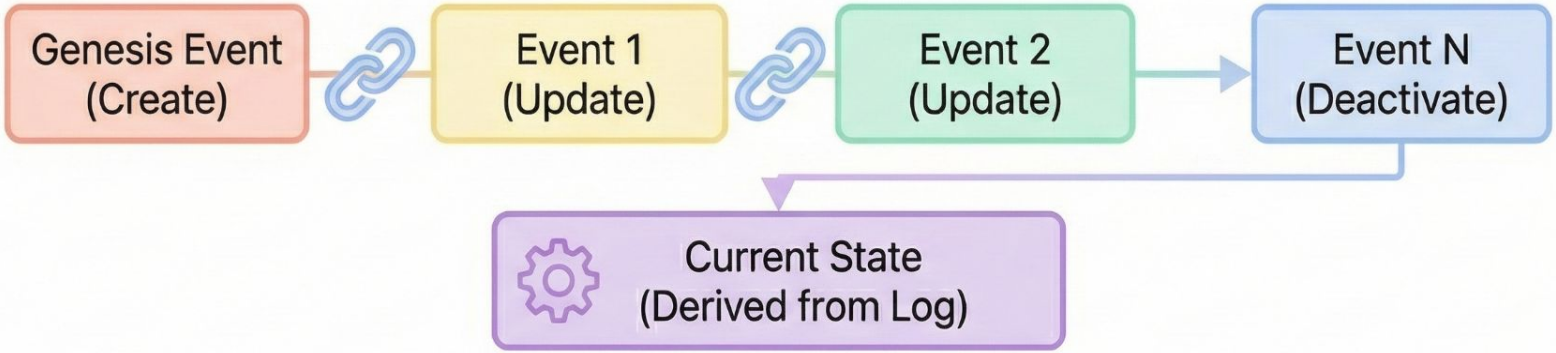
Host on simple file storage.

Near-Zero Cost

Accessible to anyone with internet.

Structured History via CEL: The Foundation

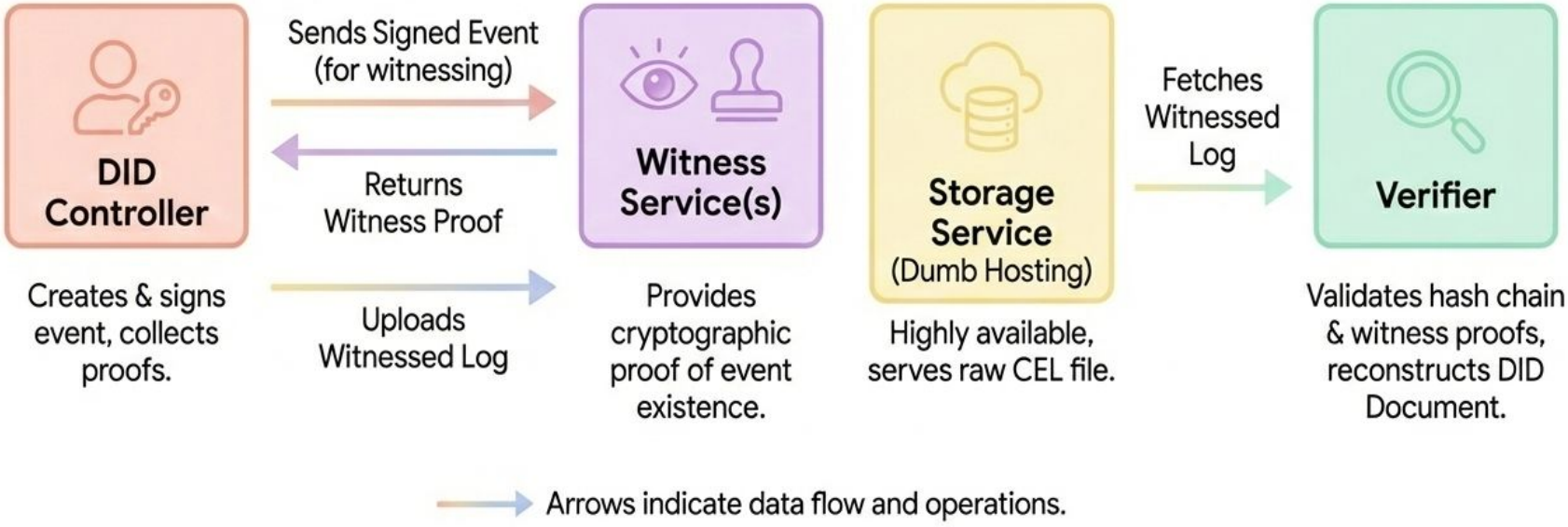
did:cel uses an append-only, tamper-evident log, not a direct DID Doc state.



Append-Only: Immutable history; no deletions or modifications.
Tamper-Evident: Cryptographic links reveal any alteration.
State Derivation: Current DID Doc is computed from the entire log.

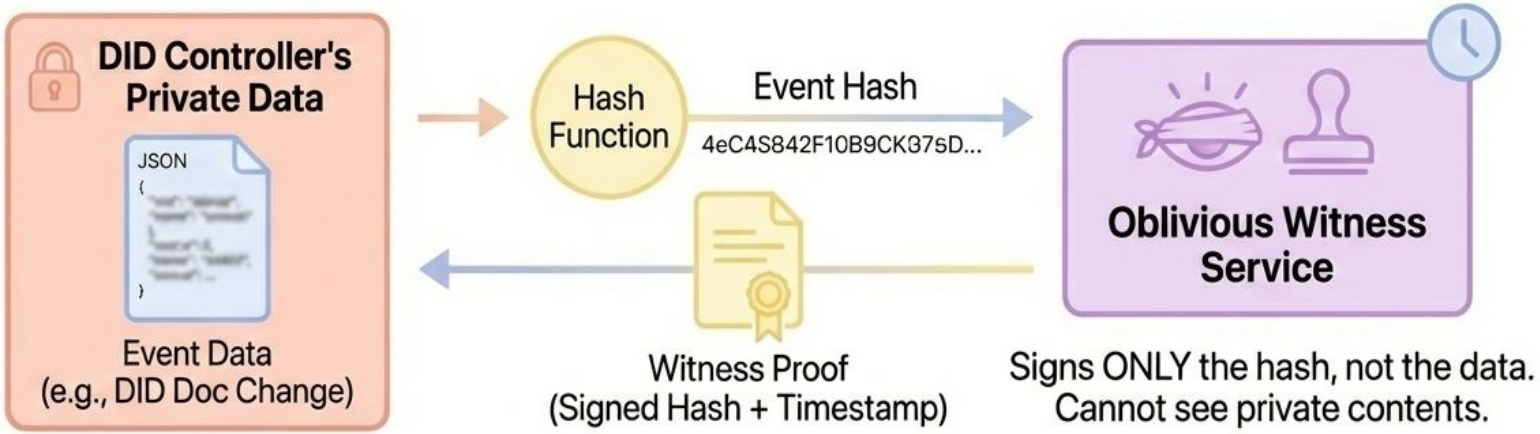
How did:cel Works in Practice: Ecosystem Overview

Witnessing and separation of concerns ensure resilience and decentralization.



Preventing History Rewrites with Witnesses

Oblivious witnessing preserves privacy while ensuring ordering and integrity.



Privacy-Preserving: Actual event data remains private to the controller.

Tamper-Evident: Ensures events are ordered and cannot be retroactively modified.

Ensuring Liveliness: The Purpose of Heartbeats

Preventing freezing, rollback, and forking by attackers.

Prevents Freezing

Attacker hides new events, showing an old log state.

Prevents Rollback

Attacker reverts the log to a previous, valid state.

Prevents Forking

Attacker creates an alternate, conflicting history.

Heartbeat Mechanism

Periodic, lightweight events added by the Controller. Proves the log is active and the latest version is being served, defeating attacks.

Looking Ahead: Robustness & Recovery

Evolving the specification for advanced security and resilience.

DNS Independence

Reduce reliance on DNS for locating storage to harden censorship resistance.

Key Pre-rotation

Explore commitment schemes for future keys to protect against quantum or theft threats.

Non-Custodial Recovery

Develop standardized methods for regaining control after key compromise.

Looking Ahead: Protocol Harmonization

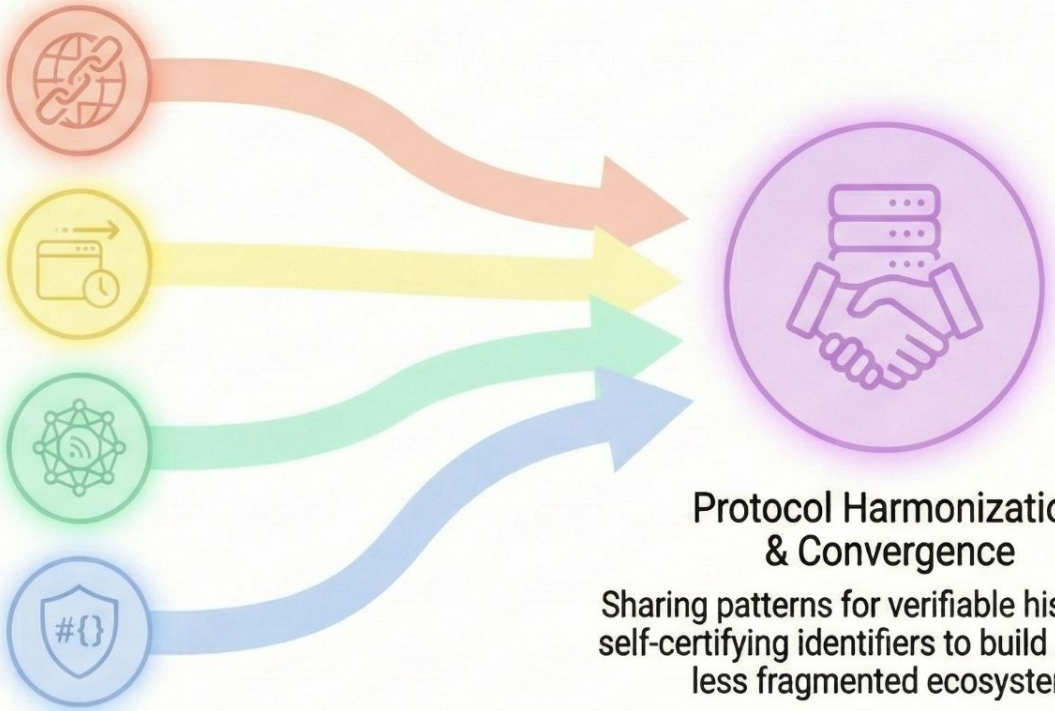
did:cel aims to align and potentially merge feature sets with other emerging standards to reduce ecosystem fragmentation.

Glogos
Harmonizing global, append-only log structures.

did:webvh
Verifiable web history patterns.

did:nostr
Decentralized social & relay protocols.

did:scid
Self-certifying identifier patterns.



Protocol Harmonization & Convergence

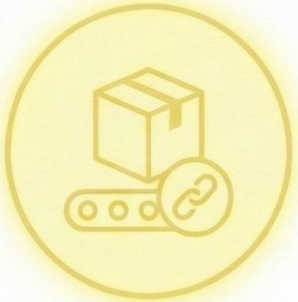
Sharing patterns for verifiable history and self-certifying identifiers to build a unified, less fragmented ecosystem.

Looking Ahead: Broader Applications of CEL

Beyond DIDs: Securing evolving data across diverse industries.

Social Networking Protocols

Tamper-evident post history, portable profiles, decentralized moderation logs.



Supply Chain Protocols

Verifiable provenance, immutable product journey, real-time audit trails.

Payment Protocols

Immutable transaction logs, transparent transparent accounting, decentralized dispute resolution.

Other Evolving Data Protocols

Any system with changing data objects needing verifiable, latest state availability.