# VeriOne

Unified Verification-as-a-Service Platform

One API. Verified Truth. Zero Bureaucracy.

Formal Proposal Document

Prepared for: Government Partners, Enterprises, Investors

## Executive Summary

VeriOne is a compliance-first Verification-as-a-Service (VaaS) platform designed to simplify and standardize access to government-backed verification mechanisms in India. By abstracting integrations with API Setu, DigiLocker, and departmental systems, VeriOne provides enterprises with a single, unified API for verification while preserving user consent, data minimization, and regulatory compliance.

The platform eliminates the need for enterprises to individually engage with multiple government bodies, reducing onboarding timelines, legal exposure, and integration complexity. VeriOne returns only verification outcomes and metadata, never raw government-issued documents or sensitive identifiers.

## 1. Problem Statement

Organizations across HR, FinTech, EdTech, and marketplace ecosystems require trusted verification of identity, education, employment, and address information. Current approaches require direct integration with multiple government APIs, each with distinct approval processes, documentation standards, and compliance requirements.

## 2. Proposed Solution

VeriOne acts as a centralized verification orchestrator. It manages user consent, routes verification requests to the appropriate government systems, enforces compliance controls, and returns standardized verification results to client platforms via a single API.

## 3. Core Principles

• Consent-driven verification bound to purpose, verifier, and time.
• Zero exposure of raw government data.
• Data minimization and auditability by design.
• Alignment with India’s Digital Public Infrastructure objectives.

## 4. Regulatory and Legal Alignment

VeriOne is designed in compliance with the Digital Personal Data Protection (DPDP) Act, API Setu usage policies, and DigiLocker consent frameworks. The platform functions as a verification orchestrator rather than a data proxy, ensuring that government data sovereignty is preserved and misuse risks are minimized.

## 5. System Architecture

Client platforms submit verification requests to VeriOne’s unified API. VeriOne initiates user consent flows, interacts with government systems through approved channels, validates responses, and discards raw data after verification. Only minimal verification metadata is retained for audit purposes.

# Technical Appendix

## A. Unified API Interface

VeriOne exposes a single verification endpoint capable of handling multiple verification types. Responses include verification status, issuer, source system, timestamp, and verification reference ID.

## B. Verification Taxonomy

Verifications are grouped into categories such as Identity, Education, Employment, Address, and Assets. Each category maps to a standardized workflow and compliance policy.

## C. Data Handling & Storage

Stored data is limited to verification identifiers, issuer metadata, timestamps, and consent references. No certificates, PDFs, or sensitive identifiers are stored.

# 6. Implementation Roadmap

Phase 1 focuses on education and identity-lite verifications. Phase 2 expands coverage to employment and address verification. Phase 3 introduces enterprise-grade features such as SLAs, dashboards, and trust scoring.

# 7. Conclusion

VeriOne enables scalable, compliant, and user-centric verification workflows that complement India’s Digital Public Infrastructure ecosystem. By centralizing complexity and enforcing strong governance, VeriOne positions itself as a trusted verification middleware for the Indian digital economy.