veridis v0.0.1

Cryptographic Verification for Real World Product Claims

Cătălin Tişca

25 February 2026

Abstract

Veridis is a cryptographic verification layer that lets suppliers across any industry prove their product claims on chain without revealing proprietary business data. Built on zero knowledge proofs, AI powered document extraction, and immutable proof anchoring, it provides a universal infrastructure for verifying origin, certifications, composition, and sourcing claims. Any Digital Product Passport platform, ERP system, consumer application, or compliance tool can integrate with a single API. This paper describes the architecture, protocol design, and rationale behind the platform.

1 Introduction

Every product label makes claims. Organic. Locally sourced. GOTS certified. Conflict free. Today, those claims are backed by PDFs, spreadsheets, and trust. A restaurant says its beef is grass fed. A fashion brand says its cotton is organic. A supplement company says its ingredients are third party tested. The supply chain behind each claim is opaque, and no one can verify it without manual audits that happen once a year at best.

The problem is structural. Suppliers hold the evidence (invoices, certificates, lab reports, spec sheets) but have no way to make that evidence verifiable without exposing confidential business data: pricing, volumes, customer lists, proprietary formulas. Brands want proof but lack the infrastructure to validate it. Regulators want compliance but lack the tooling to enforce it at scale.

The EU's Ecodesign for Sustainable Products Regulation (ESPR) will require Digital Product Passports for textiles by 2027, batteries and metals by 2028, and electronics by 2029. The Green Claims Directive will make unsubstantiated sustainability claims illegal. Food traceability laws (EC 178/2002, FSMA 204) are tightening globally. The regulatory direction is clear: every claim will need proof.

Veridis fills this gap. It is the verification layer that sits underneath Digital Product Passport platforms, compliance tools, and consumer applications. Suppliers prove claims cryptographically. Brands and regulators validate them instantly. No central authority required.

2 Use Cases

2.1 HORECA

Restaurants, hotels, and caterers make sourcing claims on every menu: local produce, organic ingredients, sustainable seafood. Veridis lets their suppliers prove each claim cryptographically. The establishment receives a verified trust badge for marketing and automated traceability

for regulatory compliance, without requiring suppliers to expose their business relationships or pricing.

2.2 Textiles and Fashion

Fashion supply chains span multiple tiers across dozens of countries. Proving that a garment's cotton is GOTS certified, its dyes are OEKO-TEX compliant, or its factory holds GRS certification currently requires manual document exchange at every tier. Veridis enables multi-tier supplier verification where each participant proves their certifications once and is trusted across the entire network. Supplier identities and commercial relationships remain private.

2.3 Any Regulated Product Category

The ESPR schedule expands into every product vertical over the next decade. Veridis does not target a single industry. The same verification infrastructure that proves a restaurant's sourcing claims proves a battery manufacturer's material composition or an electronics company's conflict mineral compliance. The regulation chooses the verticals. The infrastructure is universal.

3 Architecture

Veridis is structured as a layered stack. Each layer builds on the one below it and exposes a clean interface to the one above.

Layer	Responsibility
Universal API	REST and GraphQL endpoints for proof generation, validation, and supplier status queries. Single integration point for all consumers.
Proof Engine	Generates and verifies zero knowledge proofs. Compiles supplier evidence into circuits, produces proofs, and validates them against on chain anchors.
Data Ingestion	AI powered extraction pipeline. Parses invoices, certificates, spec sheets, and safety data sheets. Normalizes data into structured claim objects ready for proof generation.
Anchor Layer	On chain proof anchoring. Timestamps and stores proof commitments on a public blockchain. Provides immutable, auditable verification records.
Supplier Registry	Identity and credential management. Suppliers register once, submit evidence once, and are verified across all connected platforms.
Policy Engine	Configurable verification rules per industry, regulation, and claim type. Defines what constitutes valid proof for each context.

4 Zero Knowledge Verification

The core innovation is the use of zero knowledge proofs to verify supplier claims without revealing the underlying data. A zero knowledge proof allows one party (the prover) to convince another party (the verifier) that a statement is true without revealing any information beyond the truth of the statement itself.

In the context of Veridis, a supplier can prove that their product is certified organic without revealing which certifying body issued the certificate, what volume they produce, or who their customers are. They can prove that their ingredients originate from a specific country without revealing their supplier relationships or purchase prices.

The proof generation pipeline works as follows:

1. The supplier submits evidence documents (certificates, invoices, lab reports) to the data ingestion layer.
2. The AI extraction pipeline parses and normalizes the documents into structured claim data.
3. The proof engine compiles the claim data into an arithmetic circuit specific to the claim type.
4. The prover generates a zero knowledge proof attesting to the claim's validity.
5. The proof is anchored on chain with a timestamp and commitment hash.
6. Any verifier can validate the proof against the on chain anchor without accessing the original documents.

The supplier's raw data never leaves their control. Only the proof, a compact cryptographic object, is shared and stored.

5 AI Powered Data Ingestion

Suppliers already have the evidence. It exists as PDF certificates, scanned invoices, Excel spec sheets, XML safety data sheets, and email attachments. The barrier to verification has never been the absence of data. It has been the cost of structuring it.

Veridis uses AI document extraction to eliminate manual data entry entirely. The ingestion pipeline supports:

- PDF certificates of conformity (GOTS, OEKO-TEX, GRS, ISO, USDA Organic)
- Commercial invoices with line item extraction
- Laboratory test reports and safety data sheets
- Customs declarations and bills of lading
- Structured data exports from ERP systems

Documents are processed through a multi-stage pipeline: optical character recognition for scanned documents, layout analysis for structured extraction, entity recognition for identifying claim relevant data points, and normalization into the Veridis claim schema. The pipeline is designed to handle the messy reality of global supply chain documentation without requiring suppliers to change how they work.

6 On Chain Proof Anchoring

Every verified claim produces a proof that is anchored on a public blockchain. The anchor consists of a commitment hash (binding the proof to the specific claim and evidence), a timestamp, the claim type and scope, and the supplier's pseudonymous identifier. The anchor does not contain any supplier data, document contents, or business information. It contains only enough information to verify that a specific proof was generated at a specific time for a specific claim type.

Any party with the proof can validate it against the on chain anchor. This includes brands integrating via the API, DPP platforms pulling verified supplier data, regulators running compliance checks, and consumers scanning a QR code on a product label. Validation is instant, permissionless, and requires no trust in Veridis as an intermediary.

7 Universal API

Veridis does not compete with Digital Product Passport platforms, ERP systems, or consumer applications. It makes them trustworthy. The Universal API is a single integration point that any system can use to:

- Request proof generation for a supplier's claims
- Validate an existing proof against its on chain anchor
- Query a supplier's verification status and history
- Subscribe to verification events and status changes

A DPP platform like Arianee or Circulor can pull verified claim data into product passports. An ERP system can flag unverified suppliers automatically. A consumer application can display a trust badge backed by cryptographic proof rather than a self-reported label. The API abstracts the complexity of proof generation, on chain anchoring, and zero knowledge verification into simple REST and GraphQL endpoints.

8 Supplier First Design

Existing verification systems are fragmented. A supplier certified by one platform must re-verify for every new brand, retailer, or compliance tool that requests their data. This creates friction, cost, and delays that fall disproportionately on the smallest suppliers who can least afford them.

Veridis inverts this model. A supplier connects once, submits their evidence once, and receives cryptographic verification that is recognized by every brand and platform on the network. When a new brand requests verification, the supplier does not re-submit documents or undergo a new audit. The existing proofs are already on chain, already validated, and already available through the API. The marginal cost of serving one more verifier is zero.

This design is critical for adoption. Suppliers are the bottleneck in every supply chain transparency initiative. If verification is painful for suppliers, they will resist it regardless of regulatory pressure. Veridis makes verification a one-time cost with compounding returns.

9 Differentiation

Existing tools occupy adjacent positions. DPP platforms (Arianee, Circulor, Retraced) build the passport documents. Certification bodies (GOTS, OEKO-TEX) issue the certificates. Blockchain traceability platforms (Provenance, Everledger) track product journeys. Each solves one part of the problem. None provides a universal, privacy preserving verification layer that works across industries, integrates with any platform, and lets suppliers prove claims without exposing their business.

If DPP platforms are the document, Veridis is the signature.

10 Status

The platform is in active development. Architecture design, proof system specification, API schema, data ingestion pipeline design, and brand identity are complete. The immediate focus is the zero knowledge circuit library for common claim types, the AI extraction pipeline for certificates and invoices, the on chain anchoring contracts, the REST API core, and testnet deployment. Initial pilots will target HORECA supplier verification and textile supply chain certification.