Proof of Domain Identity (PDI) Protocol — Version 1.2 (Draft)

Status

Community Draft – aligned with https://bluekey.id

Author

BlueKey ID - Jason Czarnecki

Last Updated

October 2025

1. Purpose

The Proof of Domain Identity (PDI) Protocol v1.2 establishes a universal trust and identity verification framework that links domain names, wallet addresses, and intelligent agents (AI, bots, and services) under a unified verifiable identity layer. The goal of PDI is to provide a cryptographically verifiable mechanism to authenticate digital entities—whether human, corporate, or autonomous—through their domain-based roots of trust.

PDI creates an identity fabric that connects Web2 (DNS, HTTPS, organizations) and Web3 (wallets, smart contracts, decentralized identities) with the emerging Web4 paradigm of AI agents and autonomous digital entities. By combining DNSSEC, HTTPS/TLS validation, wallet signature proofs, and optional on-chain anchors, PDI enables transparent, cross-protocol verification and measurable trust scores. It ensures that not only can a person or company prove ownership of a wallet, but AI agents, digital assistants, and smart services can also establish their authenticity, authority, and provenance in real time.

This protocol positions PDI as the 'SSL of Web3 and AI identity'—a foundational layer enabling safe, verifiable, and auditable interactions between humans, machines, and organizations.

2. Design Goals

- Unified Trust Fabric: Seamlessly bridge DNS, blockchain identity, and AI agent identity.
- Verifiable Machine Identity: Enable AI agents and bots to cryptographically prove their domain affiliation and integrity.
- Composability: Support integration across identity systems (ENS, OpenAlias, PayString, DID, VC).
- Extensibility: Modular architecture allowing new alias or identity resolvers.
- Transparency: Maintain verifiable records of all identity proofs and trust scores.
- Safety: Minimize spoofing and impersonation risks through cryptographic verification.

3. Architecture Overview

Client → API Gateway → Resolver Orchestrator → Resolver Modules → Verification Engine → Trust Score Service

1. Client/API Gateway – Public REST endpoint for humans, dApps, or AI agents to resolve and verify identities.

2. Resolver Orchestrator – Manages resolver modules concurrently and aggregates identity proofs.

3. Resolver Modules – Specialized connectors for alias systems and AI identity endpoints.

4. Verification Engine – Validates proofs across DNSSEC, HTTPS, wallet signatures, and AI attestations.

5. Trust Score Service – Computes weighted, normalized trust score (0–100).

4. Expanded AI Integration (New in v1.2)

4.1 AI Agents as Verifiable Actors
AI agents can register under a parent domain (e.g., agent.finance.acme.com) and publish a PDI record linking their domain, public key, and optional wallet. Using DNSSEC and HTTPS validation, the agent becomes a verifiable digital entity that can sign messages or perform actions with provable trust.

4.2 Machine-to-Machine Verification
PDI enables autonomous services to transact, communicate, or exchange data only with verified peers. This supports verifiable agent-to-agent payments, on-chain task execution, and cross-organization collaboration.

4.3 Proof of Deployment & Authenticity
Agents include a PDI Certificate in their metadata, allowing recipients to confirm origin, key validity, and deployment timestamp. This establishes content authenticity, provenance, and tamper resistance.

4.4 Integration with Verifiable Credentials
AI identities can use DIDs and VCs to issue, receive, or validate credentials tied to domains, wallets, or agent keys via PDI.

4.5 Example:
An autonomous research bot signs an output with its private key. The receiver verifies that its domain (bot.research.ibm.com) has a valid PDI record and score >90, confirming authenticity.

5. Trust Scoring Model

Weighted scoring across layers:

Signal	Weight
DNSSEC validation	+30
HTTPS/TLS proof	+20
Wallet signature verified	+20
On-chain anchor	+15
Agent attestation verified	+10
Historical stability	+5
Failure or mismatch	-penalty

6. Security & Verification Principles

- All identities validated via DNSSEC or cryptographic key binding.
- HTTPS validation required for Web2 sources.
- AI agents sign messages using registered domain-linked keys.
- Optional on-chain anchoring provides tamper-proof persistence.
- No private key storage in DNSUSD or PDI systems.

7. Application Examples

- Human users proving wallet ownership via DNS records.
- Companies verifying employee AI assistants via domain-linked certificates.
- Autonomous bots conducting on-chain trades through PDI-verified keys.
- Cross-domain machine communication requiring PDI-based authentication.
- Regulators auditing provenance and integrity of AI-generated content.

8. Future Directions (v1.3+)

- Native AI-to-AI credential exchange using zero-knowledge proofs.
- Hardware identity integration (TPM or enclave-signed PDI records).
- PDI as default trust layer for decentralized AI networks.
- Domain-level trust metrics aggregated for predictive security intelligence.